Incident Overview

Incident Name: Ransomware Attack on Company Network

Date & Time: Monday, February 17, 2025, at 8:45 AM

Duration: Approximately 6 hours before containment efforts were fully in place

Reported By: IT Helpdesk Analyst after multiple employees reported being locked out of their files

Summary:

Description

The incident at VATI Financial Services was a devastating ransomware attack that disrupted business operations and left employees unable to access their critical files. The attackers infiltrated the system through a phishing email, planting a dormant ransomware payload that activated over the weekend. Once triggered, the malware encrypted files across the network, renaming them with a "locked" extension and displaying a ransom note demanding 50 Bitcoin in exchange for decryption. Security logs revealed unauthorized remote access from an unfamiliar IP address, suggesting the attacker had gained a foothold in the network well before deploying the ransomware. To make matters worse, the attackers also encrypted the company's backup systems, significantly complicating recovery efforts. The attack highlighted critical vulnerabilities in the organization's security posture, emphasizing the need for stronger defences against phishing, unpatched systems, and privilege escalation.

Business Impact

This ransomware attack had a significant impact on the company, listed below are some of the affected parties.

- **Clients:** Customers were unable to access their financial records or transactions due to system downtime. This might led to frustration, loss of trust, and a potential risk of loosing clients.
- **Operations:** Employees were locked out thus disrupting workflow and delaying key financial processes.
- **Backup:** With backup systems also compromised, recovery efforts became more complex, increasing downtime.
- **Services:** The disruption in systems led to delays in transactions, customer support, and internal communications. Regulatory obligations may also have been affected, potentially exposing the company to legal or compliance risks

This incident not only caused immediate operational setbacks but also posed long-term reputational and financial risks for the organization. Strengthening cybersecurity defenses will be crucial to restoring trust and preventing future attacks.

Incident Timeline

Initial Detection:

The incident was first detected on Monday morning when employees attempted to access their files and discovered they were encrypted with a "locked" extension. Additionally, multiple ransom notes demanding payment in Bitcoin appeared across affected systems. IT staff immediately escalated the issue after noticing widespread file inaccessibility

Key Actions Taken (Chronological Order)

1. **Incident Identification & Containment**
    - Employees reported being unable to access files, prompting an immediate IT investigation.
    - IT isolated affected computers and servers to prevent the ransomware from spreading further.
2. **Threat Analysis & Initial Response**
    - Security logs were reviewed, confirming unauthorized access and malware execution over the weekend.
    - Network access for compromised accounts was revoked, and suspicious connections were blocked.
3. **Eradication & System Assessment**
    - Affected endpoints were quarantined for forensic investigation.
    - The IT team attempted to restore backups, but discovered they had also been encrypted.
4. **Recovery & Restoration**
    - Systems were gradually restored using available clean backups and alternative recovery solutions.
    - Employees were instructed to reset credentials and follow strict security measures before reconnecting to the network.
5. **Post-Incident Measures & Strengthening Defences**
    - Security vulnerabilities were patched, and additional monitoring tools were implemented.
    - A cybersecurity awareness campaign was launched to educate staff on phishing risks.
    - A revised incident response plan was developed to improve preparedness for future threats.

Resolution

To fully resolve the incident, the organization took several strategic steps:

- **Rebuilding IT Infrastructure:** Since backups were compromised, clean systems were set up from scratch, ensuring no remnants of the ransomware remained.
- **Implementing Stronger Security Measures:** Multi-factor authentication (MFA) was enforced to prevent unauthorized access, and endpoint detection tools were enhanced.
- **Network Segmentation:** Systems were restructured to limit access between critical and non-critical networks, reducing future attack surfaces.
- **Incident Documentation & Compliance Reporting:** A full report was prepared, and any required legal or regulatory notifications were made.
- **Ongoing Monitoring & Testing:** Continuous security monitoring was set up, and regular penetration testing was scheduled to identify and fix vulnerabilities.

Root Cause Analysis

Primary Cause:

The primary cause of the ransomware attack was an employee unknowingly interacting with a phishing email that contained a malicious attachment. Once opened, the malware executed in the background, giving the attacker access to the company's network. This allowed them to deploy ransomware, encrypt files, and demand payment for decryption.

Contributing Factors:

Listed below are the contributing factors

- **Limited Employee Awareness:** The lack of phishing awareness training for employees made employees more vulnerable to social engineering tactics.
- **Unpatched Security Vulnerabilities:** The attacker exploited an outdated system that had not received necessary security updates, providing an entry point for the ransomware.
- **Inadequate Access Controls:** The network was not properly segmented, allowing the ransomware to spread rapidly and encrypt a large portion of company data.
- **Compromised Backups:** The backup system was not isolated from the main network, leading to backup files being encrypted as well, which complicated recovery efforts.

Discovery Method:

The root cause was identified through a series of investigative steps:

- **Reviewing User Activity Logs:** IT teams analysed login attempts and access records, revealing unauthorized access that preceded the attack.
- **Email Security Analysis:** The phishing email was traced back to an external sender, confirming it as the initial attack vector.
- **Forensic Examination of Affected Systems:** Security specialists analysed the impacted machines, identifying the specific ransomware strain and how it spread.

- **Network Traffic Monitoring:** Abnormal data transmissions were detected, linking the incident to external command-and-control servers used by the attacker.

Impact Assessment

Affected Services & Systems:

The ransomware attack disrupted several critical services and systems within the organization and they are:

- **File Servers & Databases:** Important financial records and customer data were encrypted, making them inaccessible.
- **Email & Communication Platforms:** Internal communication was severely impacted as employees couldn't access their emails.
- **Financial Transaction Systems:** Payment processing and other financial operations were delayed due to system downtime.
- **Backup & Recovery Systems:** The attackers managed to encrypt on-site backups, limiting the company's ability to restore lost data quickly.

Business Impact:

The attack had severe consequences for the organization, including:

- **Operational Downtime:** The company's services were unavailable for an extended period while IT teams worked on containment and recovery.
- **Financial Losses:** Revenue was lost due to business disruption, and additional costs were incurred for cybersecurity experts and recovery efforts.
- **Regulatory & Compliance Risks:** Depending on data protection laws, the company may face penalties for the breach, especially if sensitive customer data was exposed.
- **Reputational Damage:** Trust in the company was shaken, leading to potential loss of clients and future business opportunities.

Client Impact:

- **Access Issues:** Customers were unable to access their accounts or perform transactions while systems were offline.
- **Data Security Concerns:** Clients were worried about whether their personal and financial information had been compromised.
- **Loss of Trust:** Many customers expressed frustration over the delay in service restoration, and some may have considered switching to competitors.

- **Potential Number of Affected Clients:** While exact figures depend on the company's size and customer base, a significant portion of active users likely experienced disruption.

Response & Recovery

Immediate Response:

As soon as the ransomware attack was detected, the IT team took quick action to contain the threat. Infected systems were immediately disconnected from the network to prevent the malware from spreading further. Employees were instructed to stop using affected devices, and the security team began investigating the scope of the attack. Access to compromised accounts was revoked, and firewall rules were updated to block suspicious connections.

Short-Term Fixes:

To minimize damage and restore some level of functionality, the following temporary measures were implemented:

- **System Isolation:** All infected machines were removed from the network to prevent further encryption of files.
- **Manual Data Access Restoration:** Efforts were made to recover unaffected files and provide employees with alternative workstations.
- **Incident Communication:** Internal teams and stakeholders were informed about the attack, and guidance was given on safe computing practices.
- **Basic Security Reinforcements:** Additional security monitoring was enabled, and emergency patches were applied to vulnerable systems.

Post-Incident Review & Long-Term Fixes:

After containing the attack, a thorough post-incident review was conducted to understand how the ransomware infiltrated the system and what security gaps needed to be addressed. Permanent fixes were put in place to strengthen defences and prevent future incidents, including:

- **Enhanced Employee Training:** Company-wide cybersecurity awareness programs were introduced to help employees recognize phishing emails and social engineering tactics.
- **Stronger Access Controls:** Multi-factor authentication (MFA) was implemented to reduce unauthorized access risks.
- **Regular Security Updates:** A strict patch management policy was enforced to ensure that all software and systems remain updated.

- **Improved Backup Strategy:** Backups were moved to an offline, secure location to prevent them from being encrypted by malware.
- **24/7 Security Monitoring:** Continuous threat detection systems were deployed to identify suspicious activity before it escalates.

Communication Plan

Internal Communication:

Once the attack was detected, the IT team quickly alerted key departments through email and internal messaging platforms. Employees were instructed to disconnect from the network to prevent further spread. An emergency meeting was held to assess the situation and coordinate next steps. Updates were sent out at regular intervals to keep management and employees informed about recovery efforts.

External Communication:

External communication was more sensitive, as the company needed to balance transparency with maintaining trust. Customers were informed via email about potential service disruptions, while an official notice was posted on the website. Partners and vendors were also contacted to check if they were affected. Since this was a cybersecurity incident, legal and regulatory bodies were also notified to ensure compliance with industry standards.

Findings

What Went Well:

- **Fast Action by IT Team:** As soon as suspicious activity was reported, IT teams acted quickly to contain the issue.
- **Good Internal Coordination:** Different departments worked together efficiently, helping to limit downtime.
- **Clear External Messaging:** The company managed to communicate the issue without causing unnecessary panic.

Needs Improvement:

- **Better Employee Awareness:** The fact that the attack started with a phishing email shows that employees need more training on recognizing scams.
- **Stronger Backup Protection:** Some backups were also encrypted, making recovery harder than expected.

- **Quicker Detection:** The ransomware had already spread before it was noticed, so early detection needs improvement.

Preventative Measures:

- **Regular Cybersecurity Training:** Employees need more hands-on training on spotting phishing attempts.
- **Stronger Backup Strategy:** Backups should be stored separately to prevent them from being affected in an attack.
- **Better Monitoring Systems:** More advanced threat detection tools should be implemented to catch attacks earlier.
- **Tighter Access Controls:** Employees should only have access to the data and systems necessary for their roles.
- **Routine Security Audits:** Regular security checks can help find and fix vulnerabilities before attackers exploit them.

Action Items

Task List:

Based on the findings from the incident, listed below are the steps need to be taken to improve security and prevent future attacks:

- **Enhance Employee Training:** Conduct regular phishing awareness programs.
- **Strengthen Backup Systems:** Ensure backups are stored offline and regularly tested.
- **Improve Threat Detection:** Deploy better monitoring tools for faster attack detection.
- **Enforce Access Controls:** Limit employee access to only necessary files and systems.
- **Conduct Security Audits:** Schedule routine checks to identify vulnerabilities.
- **Patch Vulnerabilities:** Ensure all software and systems are regularly updated.

Task Assignments:

- **IT Security Team:** Implement new monitoring tools and update security protocols (**Due: Ongoing**).
- **HR & Training Department:** Organize cybersecurity awareness sessions for employees (**Due: Within 30 days**).
- **Backup Administrator:** Review and improve the backup system to prevent encryption by ransomware (**Due: Within 2 weeks**).
- **Network Administrator:** Restrict access permissions and segment the network (**Due: Within 1 month**).
- **Compliance Team:** Ensure legal and regulatory requirements are met (**Due: As per regulatory deadlines**).

Task Status:

- Enhance Employee Training – Pending
- Strengthen Backup Systems – In Progress
- Improve Threat Detection – In Progress
- Enforce Access Controls – Pending
- Conduct Security Audits – Pending
- Patch Vulnerabilities – Complete

By following these steps, the organization can reduce security risks and improve its overall incident response strategy.

Review Conducted By: Muritala Ajarat Abiodun

Date of Review: Wednesday, February 19, 2025

Incident Manager Name: Muritala Ajarat Abiodun

Incident Manager Signature: MAA

Date: February 19, 2025