MacroSoft™
An ISO 9001:2015 Company

CASE STUDY

Real-life Ransomware Story - Lessons from the Frontlines

Authors

Scott Kalcic
Chief Security Officer

Todd Gerovac
Sr. Security Consultant

Introduction

In the ever-evolving landscape of cybersecurity, ransomware attacks have emerged as one of the most formidable threats to businesses worldwide. These attacks can cripple operations, compromise sensitive data, and inflict significant financial damage. In this case study, we delve into a real-life ransomware incident faced by a shipping and transportation company, a client of Macrosoft for over 16 to 18 years. This case study aims to analyze the occurrence, response, and measures taken to address the ransomware event, providing actionable insights for similar organizations.

Incident Description

The ransomware event unfolded outside of regular working hours. The Senior IT Director was alerted when a frantic user reported missing files and non-functional systems. As multiple calls followed, it became clear that this was a widespread issue. Immediate checks revealed that the company's external connections, including its website and webmail, were down. However, the VPN remained operational, allowing access to internal servers and confirming that all files were encrypted, thus corroborating an active ransomware attack.

Actions Taken

Initial Response:

- *Verification of Incident:* The Senior IT Director began by verifying the scope of the problem, confirming that critical external services such as the website and webmail were down.
- *VPN Access:* Noted that the VPN was still operational, which facilitated remote access to internal servers for further investigation.
- *Confirmation of Ransomware:* Upon accessing internal servers, it was confirmed that all files were encrypted, indicating a full-scale ransomware event.

Containment Measures:

- *Server Shutdown:* As a precautionary measure, core servers and services that had not been affected were shut down to prevent further spread.
- *Network Quarantine:* Worked with the internal networking team and ISP to quarantine parts of the network to prevent lateral movement of the malware and block external access points.
- *Disabling Compromised Accounts:* Identified that the malicious activity came through a compromised VPN account, which was immediately disabled.

Communication and Coordination:

- *Team Mobilization:* The Senior IT Director contacted key team members to include their 3rd party security vendor and disaster recovery as a service vendor initiate the incident response plan.
- *ISP Collaboration:* Coordinated with the 3rd party security and disaster recovery vendors as well as ISP to gather key event logs and other forensic data needed for a detailed investigation.
- *Internal Communication*: Kept senior management and relevant stakeholders informed about the situation and the steps being taken to address it.

Disaster Recovery Plan Activation:

- *Incident Response Plan:* Activated a previously developed incident response plan, tailored specifically for the company's environment.
- *DRaaS Utilization:* Leveraged Disaster Recovery as a Service (DRaaS) solutions that were already in place to initiate recovery procedures.
- *Backup Equipment:* Used 3rd party security vendor loaner DRaaS equipment to set up new and segregated backups of rebuilt systems, adding an extra layer of segmentation and security during incident response.

System Restoration:

- *Rebuilding of VMs:* Started rebuilding critical Virtual Machines (VMs) utilizing resources from the DRaaS environment and reattached virtual drives, ensuring they were free from compromise.
- *Offsite Backup Utilization:* Engaged the DRaaS vendor to provide a clean backup appliance, which was used to restore critical production systems.
- *Layered Recovery Approach:* Implemented multiple points of recovery to ensure redundancy and data integrity during the entire restoration process.

Forensic and Post-Incident Analysis:

- *Forensic Investigation:* Conducted a thorough forensic analysis to understand the entry point and attack method, assisted by the third party security vendor, ISP and DRaaS vendor.
- *Law Enforcement Notification:* Notified local law enforcement to comply with legal requirements and to aid in the investigation.

Enhanced Security Measures:

- *Improved Authentication:* Enhanced multi-factor authentication and tightened access controls to prevent unauthorized access. This included hardening of VPN controls as well as addition of more secure remote access methods.
- *MDR Solutions:* Implemented Managed Detection and Response (MDR) solutions for active threat management and proactive network monitoring.
- *User Awareness Training:* Conducted extensive user awareness training to educate employees on cybersecurity best practices and to prevent future incidents.
- *Policy Enhancements:* Reviewed and updated cybersecurity policies, incorporating lessons learned from the incident.

Lessons Learned

1. Pre-incident Planning
2. Readiness
3. Remediation

Pre-incident Planning

Incident Response Plan

A well-structured incident response plan was used as the first line of defense against ransomware attacks. This plan included:

- *Identification of Critical Assets:* Determine which systems and data are most critical to your operations.
- *Roles and Responsibilities:* Clearly define the roles and responsibilities of each team member during an incident.
- *Communication Protocols:* Establish communication channels and protocols to ensure timely and accurate information flow during an incident.
- *Response Procedures:* Develop detailed procedures for detecting, analyzing, containing, eradicating, and recovering from ransomware attacks.
- *Regular Testing and Updates:* Regularly test and update the incident response plan to ensure its effectiveness and relevance.

Disaster Recovery as a Service (DRaaS)

DRaaS is a hybrid on premise/cloud-based service that replicates and hosts physical or virtual servers to provide failover in the event of a disaster. Key benefits include:

- *Offsite Replication:* Ensures that data is replicated to a secure offsite location, providing an additional layer of protection.
- *Rapid Recovery:* Enables quick recovery of critical systems and data, minimizing downtime and business disruption. Systems are recovered in hours, rather than days or weeks.
- *Scalability:* Can be scaled to meet the needs of businesses of all sizes, from small enterprises to large corporations.
- *Cost-Effectiveness:* Reduces the need for expensive on-premises disaster recovery infrastructure and provides an off site location that can be brought live during an event.

Readiness

Initial Detection

Early detection of ransomware attacks is crucial for minimizing damage. Key steps include:

- *Monitoring and Alerts:* Implement continuous monitoring and alerting systems to detect unusual activity and potential threats.
- *User Reports:* Encourage employees to report any suspicious activity or anomalies immediately.
- *Incident Confirmation:* Quickly confirm whether an incident is a false alarm or a genuine ransomware attack.

Immediate Actions

Immediate actions taken during the initial stages of a ransomware attack can significantly impact the outcome. These actions include:

- *Isolating Affected Systems:* Disconnect affected systems from the network to prevent the spread of ransomware.
- *Shutting Down Core Servers:* Temporarily shut down critical servers that have not been affected to protect them from the attack.
- *Engaging Incident Response Team:* Mobilize the incident response team to assess the situation and initiate the response plan.

Remediation

Forensic Analysis

Forensic analysis is essential for understanding the scope and impact of the ransomware attack. Key steps include:

- *Identifying the Source:* Determine how the ransomware entered the network (e.g., compromised VPN account, phishing email).
- *Collecting Evidence:* Gather logs, files, and other evidence to support the investigation and potential legal action.
- *Analyzing Malware and Detection Response Systems:* Analyze the ransomware affected envrionment to understand its behavior, encryption methods, and potential decryption options. This included points of entry.

Backup and Recovery

Effective backup and recovery strategies are critical for restoring data and systems after a ransomware attack. Key considerations include:

- *Multiple Backup Points:* Maintain multiple backup points to ensure data integrity and availability.
- *Offsite Backups:* Store backups in a secure offsite location to protect them from local attacks.
- *Regular Testing:* Regularly test backup and recovery procedures to ensure they work as expected.

Rebuilding and Restoration

Rebuilding and restoring systems after a ransomware attack involves several steps:

- *Prioritizing Critical Services:* Focus on restoring critical services first to minimize business disruption.
- *Rebuilding Virtual Machines:* Rebuild affected virtual machines and reattach virtual drives after thorough analysis.
- *Following the DR Plan:* Adhere to the predefined disaster recovery plan to ensure a structured and efficient recovery process.

Key takeaways

Importance of a Comprehensive Plan

A comprehensive incident response and disaster recovery plan is essential for effective ransomware mitigation. Key elements include:

- *Detailed Procedures:* Develop detailed procedures for each stage of the incident response and recovery process.
- *Regular Training:* Conduct regular training sessions to ensure all team members are familiar with the plan and their roles.
- *Continuous Improvement:* Continuously review and improve the plan based on lessons learned from incidents and testing.

Enhanced Security Measures

Implementing enhanced security measures can help prevent future ransomware attacks. Key measures include:

- *Multi-Factor Authentication (MFA):* Use MFA to add an extra layer of security to user accounts.
- *Managed Detection and Response (MDR):* Deploy MDR solutions for continuous network monitoring and threat intelligence.
- *User Awareness Training:* Educate employees about cybersecurity best practices and the importance of vigilance.

Team Coordination

Effective team coordination is crucial for a successful response to ransomware attacks. Key practices include:

- *Clear Communication:* Establish clear communication channels and protocols to ensure timely and accurate information flow.
- *Defined Roles:* Clearly define the roles and responsibilities of each team member during an incident.
- *Regular Drills:* Conduct regular drills to practice the incident response plan and improve team coordination.

Conclusion

This case study provides insights into the critical aspects of responding to a ransomware attack, from initial detection to the recovery phase. By sharing this experience, Macrosoft aims to educate and prepare other businesses to face similar threats. The key takeaway is clear: proactive planning, robust security measures, and a coordinated response are essential to mitigating the impact of ransomware attacks.

For more information on how Macrosoft can assist with risk assessment, policies and procedures, awareness training, managed service programs, threat intelligence, continuous monitoring, disaster recovery, and incident response management, please visit our website or contact us directly.

MacroSoft™
An ISO 9001:2015 Company

THANK YOU !

For more information, please contact us.

Joe Rafanelli

Director of Technical Solutions

Macrosoft Inc

135 US-202/206, Suite #9

Bedminster, NJ 07921

jrafanelli@macrosoftinc.com

(973) 223-9717

www.macrosoftinc.com