AMERICAN INTERNATIONAL UNIVERSITY–BANGLADESH (AIUB)

FACULTY OF SCIENCE & TECHNOLOGY

NETWORK SECURITY

Summer 2023-2024

Section: A

Mid-Term Report

Supervised By

Md. Manirul Islam

Submitted By

Name: Irtiza Ahsan Abir

ID: 21-45009-2

Analysis of the Royal Mail Ransomware Attack of 2023

An in-depth case study on the LockBit RaaS attack

Abir Irtiza Ahsan
CSE
American International University Bangladesh
Dhaka, Bangladesh
Irtizaahsan944269@gmail.com

***Abstract*—International mail systems were disrupted by a massive ransomware outbreak that hit the UK's Royal Mail in January 2023. This article offers a thorough examination of the attack, the exploited vulnerabilities, the quick fixes, and suggestions for future mitigation. Using LockBit Ransomware-as-a-Service (RaaS), the attackers targeted a Belfast distribution facility. The attack caused significant interruptions to operations and was first linked to Emotet malware, which was discovered in November 2022. This research attempts to clarify attack techniques and provide recommendations for improving cybersecurity defenses.**

KEYWORDS

Ransomware, Cybersecurity, LockBit RaaS, Royal Mail, Emotet, Incident response

I. Introduction

In the digital age, ransomware attacks are becoming a common danger to businesses in a variety of industries. A massive ransomware assault that affected 11,500 Post Office outlets and hampered international mail services occurred against the UK's Royal Mail in January 2023[1]. This report offers a thorough examination of the attack, looking at the exploited vulnerabilities, the quick steps made in reaction, and suggestions for future mitigation techniques.

II. Attack Summary

In January 2023, the Royal Mail was hit by a ransomware attack employing the LockBit RaaS, which largely affected a distribution hub in Belfast, Northern Ireland [1][2]. This attack caused major operational difficulties, particularly in the han- dling of overseas packages.

III. Exploited Vulnerability

The Emotet malware was discovered on Royal Mail servers in November 2022, which is when the attack first started [2]. Attackers intensified their efforts by January 2023 and used the LockBit ransomware to encrypt data and steal confidential information. Affiliates of LockBit frequently take advantage of flaws in network security and use malware or phishing schemes to obtain unwanted access.

IV. Remedy Actions Taken

Following the attack, Royal Mail implemented several immediate measures to mitigate the damage:

- **System Isolation:** Infected systems were isolated to prevent further spread.
- **Incident Response:** The National Cyber Security Centre (NCSC) and other UK agencies were engaged to assist in the response.
- **Alternate Carriers:** Temporary recommendations for using alternate carriers for international deliveries were made to ensure service continuity.
- **System Restoration:** Efforts were made to restore affected systems from backups and re-secure the network infrastructure.

V. Recommended Future Mitigation Strategy

To prevent future incidents, Royal Mail and similar organizations should consider the following strategies:

- **Enhanced Cyber Hygiene:** Regular updates and patches for all systems to address known vulnerabilities.
- **Advanced Threat Detection:** Deployment of advanced threat detection and response tools to identify and mitigate threats in real-time.
- **Employee Training:** Continuous cybersecurity awareness and training programs to educate employees about phishing and other common attack vectors.
- **Multi-Factor Authentication (MFA):** Implementation of MFA for accessing critical systems to reduce the risk of unauthorized access[4].
- **Incident Response Plan:** Regular review and testing of incident response plans to ensure quick and effective action during an attack.
- **Third-Party Audits:** Regular third-party security audits to identify and rectify potential security weaknesses.

VI. Figures and Tables

TABLE I
TIMELINE OF THE ROYAL MAIL RANSOMWARE ATTACK

Date	Event
November 2022	Detection of Emotet malware on servers
January 2023	LockBit ransomware attack initiated
January 2023	Isolation of infected systems
January 2023	Engagement of NCSC and other UK agencies
January 2023	Recommendations for alternate carriers issued
February 2023	System restoration and network re-securing

ACKNOWLEDGMENT

The authors would like to thank the National Cyber Security Centre (NCSC) for their support during the incident response. Additionally, we acknowledge the contributions of Royal Mail's IT and cybersecurity teams for their efforts in mitigating the attack's impact [5].

REFERENCES

[1] Royal Mail resumes international deliveries six weeks after ransomware attack," The Guardian, Feb. 21, 2023. [Online]. Available: https://www.theguardian.com/business/2023/feb/21/royal-mail-international-deliveries-cyber-attack-ransom-strikes

[2] Royal Mail Ransomware Attack Timeline," Cyber Management Alliance, Feb. 2023. [Online]. Available: https://www.cm-alliance.com/cybersecurity-blog/royal-mail-ransomware-attack-timeline

[3] BCS, 'Biggest Cyber Attacks of 2023.' DOI: 10.9101/bcs.2023.

[4] Royal Mail Ransomware Attack - Part 2." *Pentest People Blog*, Pentest People, 2024. Available: https://www.pentestpeople.com/blog-posts/royal-mail-ransomware-attack-part-2

[5] Our Statement on the Incident Affecting [Activity]." *LinkedIn*, July 5, 2024. Available: https://www.linkedin.com/posts/national-cyber-security-centre_our-statement-on-the-incident-affecting-activity-7018974634670702592-EZNR