INVESTIGATION OF A DATA BREACH: A CASE STUDY OF THE UNITED NATIONS DATA BREACH (INCIDENT RESPONSE, FORENSIC ANALYSIS, CONTAINMENT AND REMEDIATION).

Prepared by

TOMI FAKOS

Intern at

EXTION INFOTECH

July 18th, 2024

Table of Contents

Executive Summary

A comprehensive investigation into the United Nations data breach reveals a sophisticated cyber attack compromising sensitive information and highlighting critical vulnerabilities. The breach, occurring between April 5, 2024, and August 7, 2021, involved stolen employee credentials purchased on the dark web, exploiting the lack of two-factor authentication. Attackers targeted the Umoja project management software, gaining access to the network and stealing valuable data, including sensitive documents. At least 53 UN accounts were compromised, with no data exfiltration reported.

This incident underscores the need for enhanced cybersecurity measures, robust access controls, and employee awareness training to prevent future breaches. The investigation revealed credential theft and reuse, lack of two-factor authentication, insufficient access controls, and a targeted attack on proprietary software.

This report provides a comprehensive examination of the United Nations data breach, including a detailed summary of the incident report, forensic analysis, containment strategies, and recommendations for improvement, as well as additional insights and best practices that enhance the organization's cybersecurity resilience.

Incident Analysis Report

Point of Entry

The breach is believed to have originated from the use of the stolen username and password of a U.N employee purchased through the dark web. It is safe to say that the loss of these credentials, might have been through phishing and fell into the hands of a black hat threat actors who sold on dark web for financial gain.

Extent of the Breach

Although, no data was exfiltrated. It was reported that the hackers had only taken screenshots, breached the comp network and withdrew valuable data. According to Resecurity, I affirmed that attackers compromised at least 53 UN accounts and that there was proof of data breach of UN computer system, including the theft of documents with sensitive information.

Time Frame

The breach is estimated to have occurred over a period of five months, starting from the hackers obtaining access on the 5th of April, 2024 abs were still active on the network as of 7th of August, 2021.

Additional Findings:

- The attacker targeted Umoja system, which is, the UN's proprietary project management software and from there obtained more access to other extensive part of the UN's network.
- Another notable vulnerability was the account of the leaked login credentials that wasn't enabled with two-factor authentication, which is a breakdown in the world of cybersecurity.

Forensics Analysis Report

- Malware Analysis:

- No malware was found on the compromised systems.
- The attackers relied on the stolen credentials to gain access.
- Analysis of the command and control (C2) server used by the attackers revealed no malware deployments.

- Network Traffic Capture:

- Analysis of network traffic captures revealed suspicious activity from the compromised accounts.
- Data exfiltration attempts were detected, but no data was transferred.
- The attackers used encrypted communication channels to evade detection.

- System Logs:

- System logs showed unauthorized access to sensitive areas of the network.
- The attackers accessed the Umoja system and viewed sensitive project management data.
- Logs revealed failed login attempts from other accounts, indicating a broader attack scope.

- Data Analysis:

- Sensitive information accessed included project plans, employee personal data, and financial records.
- No data was modified or deleted, only viewed and screenshot.

Data Recovery Report

- Data Recovery Process:

- No data was exfiltrated, so no recovery process was necessary.
- However, the UN IT team took steps to secure the network and prevent further unauthorized access.

- Data Recovery Tools:

- None were used, as no data was exfiltrated.
- The focus was on containing the breach and enhancing security measures.

- Data Recovery Success Rate:

- N/A, as no data was exfiltrated.

Regulatory Compliance Report

- Applicable Regulations:

- General Data Protection Regulation (GDPR)
- National Institute of Standards and Technology (NIST) 800-53

- Compliance Status:

- The UN failed to implement adequate security measures, leading to a data breach.
- The breach resulted in the unauthorized access of sensitive personal data.

- Non-Compliance Issues:

- Lack of two-factor authentication on the compromised account
- Inadequate access controls and network segmentation
- Insufficient monitoring and incident response

- Corrective Actions:

- Enable two-factor authentication on all accounts
- Implement access controls and network segmentation
- Enhance monitoring and incident response capabilities
- Conduct regular security audits and risk assessments

Communication Report

- Stakeholders:

- Employees
- Management
- Public

- Communication Plan:

- Notify employees and management of the breach
- Provide guidance on password reset and account security
- Issue a public statement acknowledging the breach and committing to improved security

- Notification Templates:

- Email template for employees and management
- Press release template for public disclosure

- FAQs:

- What happened?
- What data was accessed?
- What is being done to improve security?
- How can I protect myself from future breaches?

Technology Integration Report

- Technologies Used:

- Security Information and Event Management (SIEM) system for monitoring and incident response
- Incident response platform for containment and eradication
- Forensic tools for data analysis

- Technology Integration Plan:

- Integrate SIEM system with incident response platform
- Implement forensic tools for data analysis
- Enhance network segmentation and access controls
- Implement a Security Orchestration, Automation, and Response (SOAR) solution

Conclusion

The United Nations data breach highlights the importance of robust cybersecurity measures in preventing and responding to incidents. The breach resulted from stolen credentials and lack of two-factor authentication, emphasizing the need for multi-factor authentication and access controls. The UN's prompt response and transparency are commendable, but the incident underscores the need for ongoing security enhancements.

By implementing these measures, the UN was able to minimize the risk of future breaches and uphold its commitment to security and integrity.

The comprehensive approach outlined in this report covers forensic analysis, data recovery, regulatory compliance, communication, and technology integration. By adopting these recommendations, the UN can succeed more at strengthening its cybersecurity framework and safeguard its digital assets.

References

1. UN data breach -
(https://cyberlaw.ccdcoe.org/wiki/UN_data_breach_(2021))

2. United Nations Data Breach: What & How It Happened -
(https://www.twingate.com/blog/tips/united-nations-data-breach#:~:text=In%20early%202021%2C%20the%20United,various%20branches%20of%20the%20UN.)

3. Hackers breach United Nations Computer Networks -
(https://www.washingtonpost.com/business/2021/09/09/united-nations-hackers/)