Incident Report 2025-11-11

Title:
Date:
Alert Type/Category:
Severity: Low / Medium / High / Critical
Analyst Name:
Case #:

DETECTION AND ANALYSIS

Alert Summary:

The user acount lars.haugen was observed uploading large amounts of data to DropBox between 2025-10-29 07:59:00 and 2025-10-29 08:35:08 from the host WIN10-DH-113. The data According to Microsoft Defender for Cloud Apps the data volume exceeds 1.1GB, but we have no data on the total size of the uploaded data.

Prior to the upload activity we observe use of the tool “rclone.exe” in the EDR logs, which is a tool designed for synchronising files to cloud storage [1]. The command line used is the following:

rclone copy C:\Users\Lars\Documents\Finance dropbox:/Finance_Backup

This indicates that the tool was used to transfer the contents of C:\Users\Lars\Documents\Finance to DropBox. This could be part of your organisation’s legitimate backup solution, but the use of DropBox for data exfiltration is common among malicious adversaries and the app is unsanctioned according to Microsoft Defender for Cloud Apps.

This is especially suspicious as the account was observed attempting to attach sensitive files to an email composed with the recipient “lars.personal@gmail.com”. The first attempt attempted to attach the file “Q3_Financials.xlsx”, which was blocked by a DLP policies that detected attempts to send Sensitive PII and Confidential data. The user account then attempted to send an email with the attachment “Client_Contracts_Archive_pwd.zip”. Also this was blocked by transport rules indicating that this was an attempt to exfiltrate data in a password protected archive file.

References

[1] https://rclone.org/

Key Details:

User account: lars.haugen@datahaven.no
Email recipient: lars.personal@gmail.com
Email subject: Q3 docs
Email attempted attachements:
- Client_Contracts_Archive.zip
- Q3_Financials.xlsx

- Client_Contracts_Archive_pwd.zip
Command line: rclone copy C:\Users\Lars\Documents\Finance\ dropbox:/Finance_Backup

Consequence:

This could indicate that an malicious actor has managed to send sensitive documents outside of the organisation's infrastructure, which could be leveraged for extortion, sold to competitors, or leaked to reduce competitiveness.

CONTAINMENT

Executed Remediation Actions:

- Isolated the host WIN10-DH-113

Recommended Remediation Actions:

- Determine the nature of the exfiltrated data
    - The detections indicate that the documents contain sensitive PII, consider if this is a breach of GDPR
- Determine if this activity is known to the user
    - If the user performed this action, investigate why and if this was malicious
    - Consider disabling the user account and persecution of the user
- If unknown the user account should be considered compromised
    - Disable the user and revoke any active sessions
    - Investigate available logs to determine how and when the user account was compromised