

A stolen session became domain administrator in 41 hours

*Between 14 and 16 September an intruder moved from one finance mailbox to the domain controller of Meridian Freight. **Nothing in the path was an exploit: every step used access that was already allowed.** The intruder was removed before any data left the network.*

Prepared by Hunt & Hackett Incident Response for the CISO of Meridian Freight. 2 October 2026.

The intruder was fast at the end and patient in the middle

The whole intrusion took two days. Three quarters of that time was spent on one workstation, waiting for an administrator to sign in.

First access to domain administrator

41 hours

14 September 08:12 to 16 September 01:20

Detection to containment

5.5 hours

alert at 01:50, accounts disabled by 07:20

Systems the intruder used

5

of 1,840 in the domain

Largest outbound transfer

4 MB

no sign that data was taken

This report sets out the path the intruder took, the evidence for each step, why none of it raised an alarm for 41 hours, and the three changes that would have stopped it.

Five hops from a mailbox to the domain controller

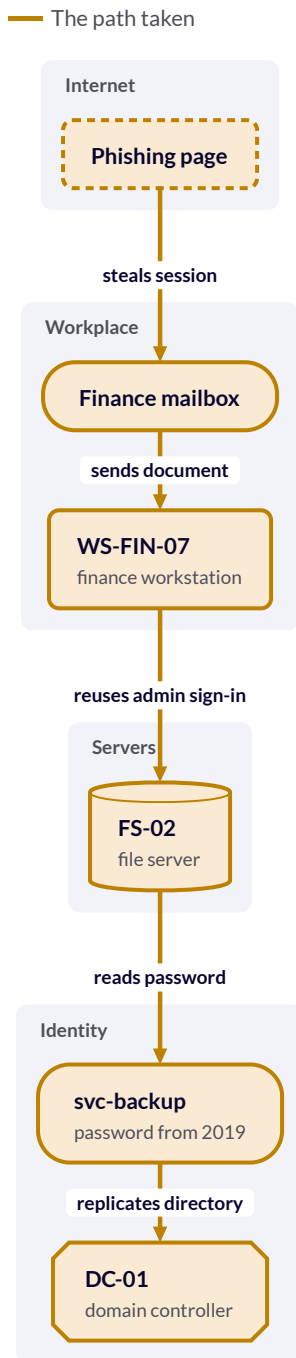
Each hop used a credential that the previous system handed over.

The five steps below take them one at a time.

Figure 1

Each hop used access the last one had earned

Path of the intrusion, by network zone



Source: mail, endpoint and directory logs, 14 to 16 September 2026.

Hour 0. A session is stolen

A finance clerk signs in on a page that looks like the company portal. The page relays the login to the real one, including the code from the authenticator app, and keeps the session cookie.

Eleven minutes later the same session is used from an address in another country.

Hour 2. A colleague opens a document

From the clerk's mailbox the intruder replies to a real thread with a spreadsheet. It comes from a known sender, about a known invoice, so a colleague opens it and enables its content.

The macro starts a remote-access tool on workstation WS-FIN-07.

Hour 32. An administrator signs in

For thirty hours the tool does nothing but check in. Then a file-server administrator signs in to WS-FIN-07 to fix a printer, and the intruder copies that sign-in from memory.

Hour 38. A password is found in a script

With the administrator's sign-in the intruder browses file server FS-02 and finds a backup script. The script holds the password of the account svc-backup in plain text. The password was set in 2019.

Hour 41. The directory is theirs

The backup account may replicate the directory. The intruder uses it to request the password data of every account, which is the same as holding the domain.

That request is the first thing in the whole path that raised an alert.

Forty-one hours unseen, then five and a half to contain

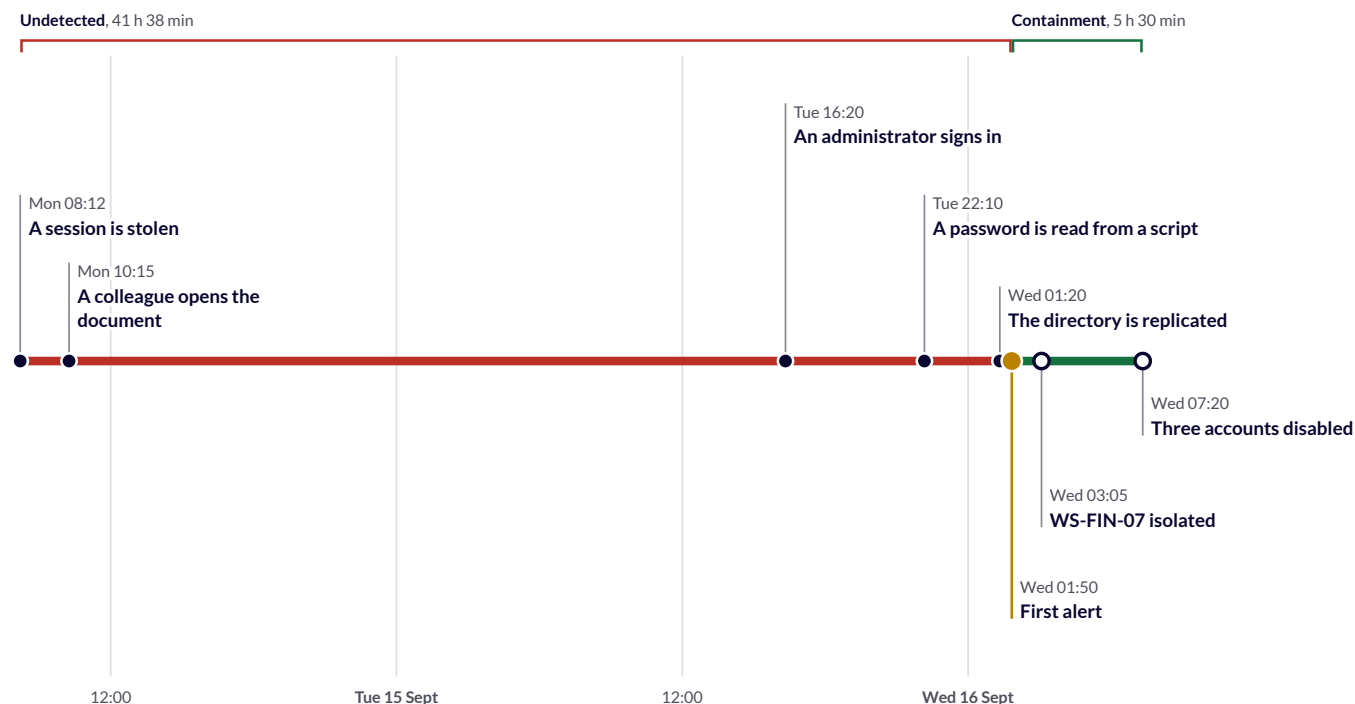
The line below is to scale. Above it is what the intruder did; below it, what the response did. Almost all of its length is the time before anyone knew.

Figure 2

The intruder went unseen for 41 hours and was removed within six

The intrusion and the response, 14 to 16 September 2026, times in UTC

● Intruder ○ Response



Source: mail, endpoint and directory logs, and the responders' own log.

Thirty of those hours passed on one workstation

The intruder touched five systems. On four of them the activity lasted a few hours at most. The long bar is the wait on WS-FIN-07, and it was the best chance to catch the intrusion: a remote-access tool was checking in every ten minutes, from a finance workstation, for more than a day.

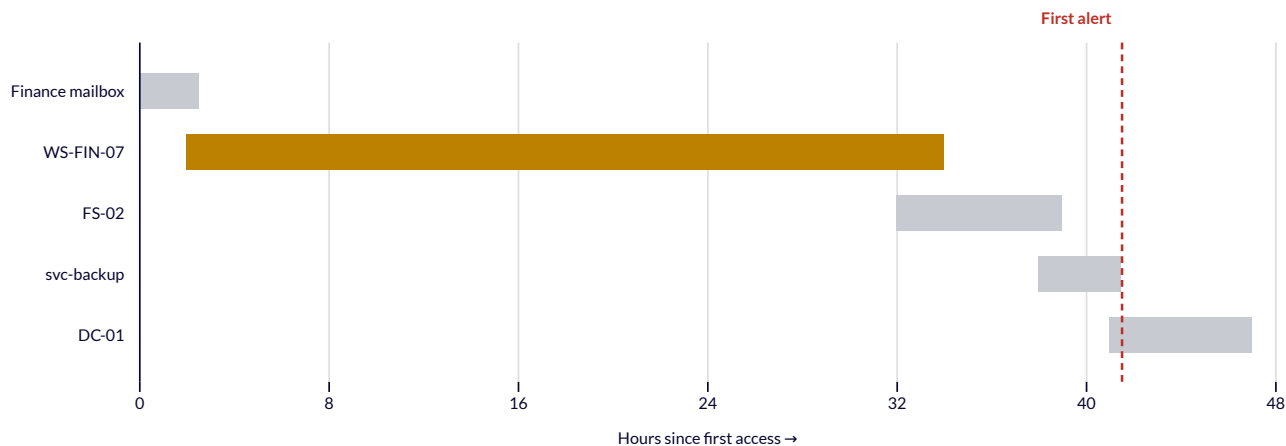
How to read it

A bar is the time the intruder was active on a system. A dot is an event on the line above. The dashed line is the first alert.

Figure 3

The wait on the workstation is most of the intrusion

Intruder activity by system, hours since first access



Source: endpoint telemetry and sign-in logs. Hour 0 is 14 September 2026, 08:12 UTC.

Three log entries carry the case

Each of the three turning points left one record that settles what happened. They are reproduced as found, shortened where marked.

```
# Sign-in log: one session, two countries, eleven minutes apart
08:12:41 j.vermeer session 7f3a...c1 NL Windows authenticator success
08:23:55 j.vermeer session 7f3a...c1 R0 Linux (token) success

# FS-02, D:\Scripts\nightly-backup.ps1, last changed 2019-03-04
$user = "MERIDIAN\svc-backup"
$pass = "..." # in plain text; removed from this report

# DC-01 security log, 16 September 01:20:07
4662 svc-backup Replicating Directory Changes All from 10.20.7.31
```

Phishing domain	portal-meridianfreight.example, registered 9 September
Relay address	203.0.113.48
Remote-access tool	finsync.exe, in the user's AppData folder, checking in every 600 seconds
Accounts used	j.vermeer, adm-dkoster, svc-backup

The five systems, and where each stands now

System	Used for	Hours	Status
Finance mailbox	Sending the document	2.5	● Sessions revoked
WS-FIN-07	Waiting for a better credential	32	● Rebuilt
FS-02	Finding the backup password	7	▲ Scripts under review
svc-backup	Replicating the directory	3.5	● Replaced
DC-01	Target	6	▲ Monitored until 16 December

Any one of three controls would have ended it

The path had five hops, and it needed all of them. Each of the measures below removes one, at a different point and at a different cost.

1

Bind sessions to the device

The stolen session would not have worked from the intruder's machine. Stops the path at hour 0.

2

Keep administrators off workstations

There would have been no better credential to wait for. Stops it at hour 32.

3

Rotate and vault service passwords

The script would have held nothing of use. Stops it at hour 38.

16 Sep	Contained	Three accounts disabled, WS-FIN-07 isolated, directory password data reset twice.
30 Sep	Service passwords rotated	All 46 service accounts; 9 scripts with passwords in them rewritten.
31 Oct	Device-bound sessions for finance and administrators	
15 Dec	Separate administration workstations in use	

Decision needed

Extend device-bound sessions from 240 people to all 2,400 by March

Finance and administrators are covered by 31 October. Every other mailbox can still be used the way this one was.

What we did not find

No outbound transfer larger than 4 MB from any of the five systems, no new accounts, no changes to group policy, and no sign of the tool on any other workstation. Mail rules on the clerk's mailbox were unchanged.

Hunt & Hackett Incident Response, 2 October 2026. An example report: Meridian Freight, the people and the events in it are invented.