

One stolen session became domain administrator in 41 hours

Nothing in the path was an exploit. **Every step used something that was already allowed.**

For the management team of Meridian Freight, 6 October 2026. The written report is IR-2026-031.

It was stopped before any data left

First access to domain administrator

41 hours

14 to 16 September

First alert to containment

5.5 hours

overnight, by the on-call team

Systems the intruder used

5

of 1,840 in the domain

Each step used access the last one had earned

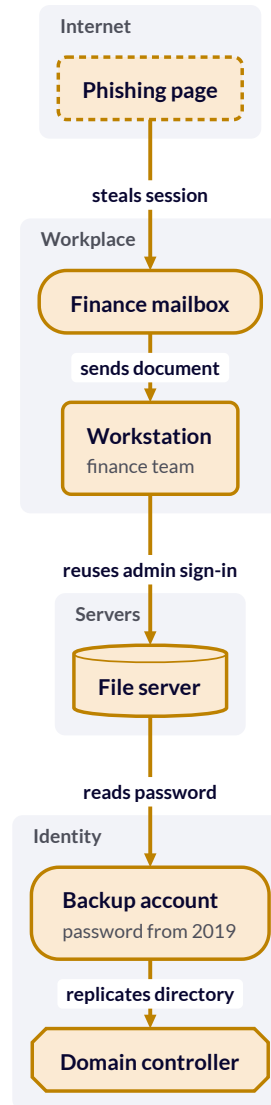
A stolen session opened a mailbox, the mailbox delivered a document, and each machine handed over the credential for the next.

Step through the path, or press Play.

Five hops from a mailbox to the domain controller

Path of the intrusion, by network zone

— The path taken



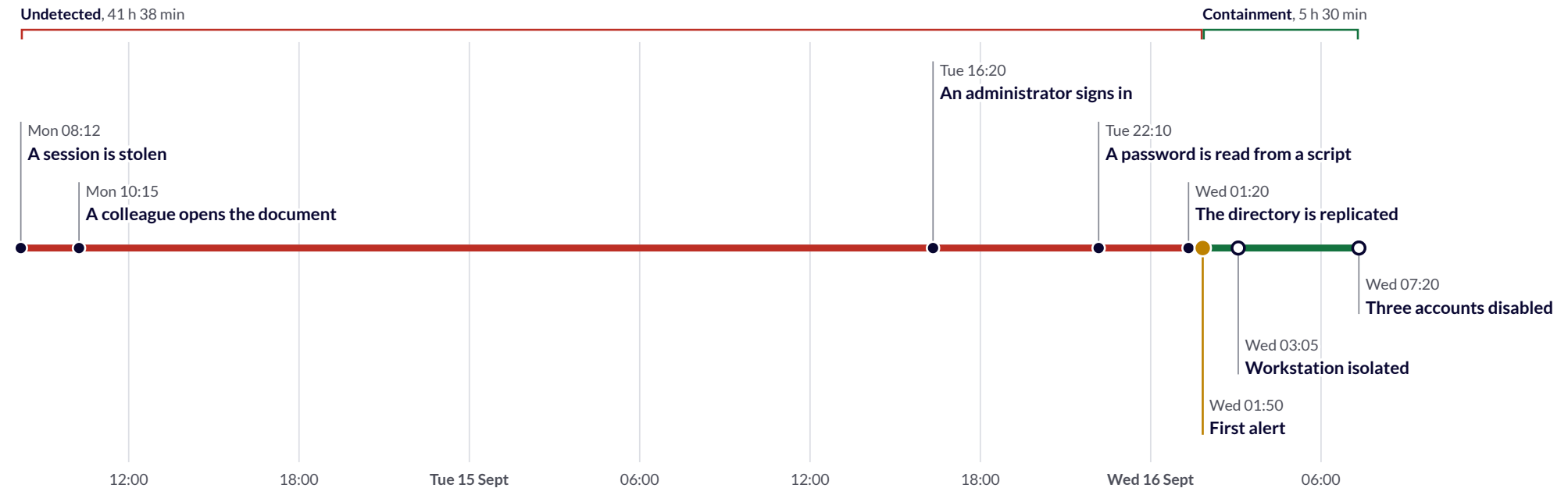
Source: mail, endpoint and directory logs.

Thirty of the 41 hours passed between two machines

Unseen for 41 hours, removed within six

The intrusion above the line, the response below it. 14 to 16 September, times in UTC

● Intruder ○ Response



Source: first activity on each system, and the responders' own log.

Nothing was broken into.
Each step was allowed.

Any one of three controls would have ended it

1

Bind sessions to the device

The stolen session would not have worked from the intruder's machine.

2

Keep administrators
off workstations

There would have been no better credential to wait for.

3

Rotate and vault service passwords

The script on the file server would have held nothing of use.

One decision for today

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.