XHack Security
Cloud
Investigation

CONFIDENTIAL — XHACK

FORENSIC INVESTIGATION REPORT

DEMO Logs

An autonomous analysis of the cloud and SaaS audit logs supplied for this incident — how the account was reached, the first moment it was used, what was done with it, and what that puts at risk.

REPORT DATE	STATUS	EVIDENCE FILES
21 Sep 2026, 00:22 UTC	Running	1
COVERAGE	**FINDINGS**	**REPORT ID**
100%	21	67c436b0-d0c9-470a-9e2e-19c75be37dd9

EXECUTIVE SUMMARY

What we found

The counts below are computed from the record, not written by the analysis.

9 critical findings

Immediate action is recommended. Start with the recommended actions below.

This investigation reached its limit on analysis steps

Every run has a ceiling on how many steps it may take, and this one reached it, so the analysis wrote up what had been proved to that point. Anything it had not yet reached is unexamined, not cleared. This is a limit on the run, not on your plan or your AI usage.

9	11	0	8
Critical	High	Medium	Indicators

100%
Evidence swept

THE ACCOUNT OF WHAT HAPPENED

A single M365 unified audit log (25,697 rows, 2026-07-15T00:03:28 to 2026-08-29T19:29:24) records a deliberate, admin-level intrusion of the acme.com tenant over 17 days. It began with a password spray against 119 accounts at 2026-07-27T03:11:00 from 198.51.100.9, moved to unauthorised mailbox access on four accounts (dana.whitfield 2026-08-03, marcus.lee 08-04, priya.raghavan 08-05, t.okafor 08-06), escalated through a backdoor admin account, a tenant-wide OAuth consent grant and mail-exfiltration rules, and ended in business email compromise. The customer's remediation on 2026-08-14 did not stop it: the attacker's OAuth application was never removed, and it read priya.raghavan's mailbox and sent fraudulent remittance mail to an external supplier through the end of the log. The intrusion is live at the last recorded event.

POINT OF ENTRY

The first moment

The earliest event that can be proved to be part of this intrusion. Everything after it is consequence.

Time not established

198.51.100.9 (unauthenticated) — Password spray from 198.51.100.9

- 240 UserLoginFailed events against 119 distinct accounts from a single source, UserAgent BAV2ROPC, LogonError InvalidUserNameOrPassword, all within 28 minutes (last 03:38:53). First event of the intrusion in the log.

RECONSTRUCTION

How it happened

The sequence in order, mapped to MITRE ATT&CK tactics. **Red** stages are attacker actions; **green** stages are detection and response.

1 STAGE FIRST MOMENT

Password spray from 198.51.100.9

by **198.51.100.9 (unauthenticated)**

- 240 UserLoginFailed events against 119 distinct accounts from a single source, UserAgent BAV2ROPC, LogonError InvalidUserNameOrPassword, all within 28 minutes (last 03:38:53). First event of the intrusion in the log.

2 STAGE

Mailbox access begins on dana.whitfield

by **198.51.100.74**

- First MailItemsAccessed on dana.whitfield@acme.com from the attacker address, 7 days after the spray; 420 mail items read by 16:15:09.

3 STAGE

Hiding rule planted on dana.whitfield

by **198.51.100.74**

- New-InboxRule moving phish/suspicious/security alert/unusual sign-in messages to Deleted Items, marking read, StopProcessingRules True. Rule named '.'.

4 STAGE

Attacker searches mailbox contents

by **198.51.100.74**

- Seven keyword searches of dana.whitfield's mailbox between 16:18:21 and 16:28:57, including a SearchQueryInitiatedExchange whose AuditData contains 'payment instructions'.

5 STAGE

marcus.lee mailbox compromised and rule planted

by **198.51.100.74**

- 106 MailItemsAccessed on marcus.lee@acme.com from 198.51.100.74 and a hiding New-InboxRule at 12:03:44. marcus.lee was never a spray target.

6 STAGE

priya.raghavan mailbox compromised and rule planted

by **198.51.100.142**

- UserLoggedIn 08:33:26, 106 MailItemsAccessed 08:39:53-09:11:56, hiding New-InboxRule at 08:51:17 named '..'.

7 STAGE

t.okafor taken over; backdoor service account created and given Organization Management

by **t.okafor@acme.com from 198.51.100.142**

- Hiding New-InboxRule, 116 MailItemsAccessed 13:09:00-13:44:32, 'Add user.' creating svc-backup-sync@acme.com at 13:19:04, 'Add member to role.' adding it to Organization Management at 13:28:47, Add-MailboxPermission at 13:35:12.

8 STAGE

Rogue OAuth application created and given tenant-wide mail access

by **t.okafor@acme.com from 198.51.100.142**

- 'Add service principal.' creates app 'ACME Mail Connector' (7b2e9a14-5c83-4d16-9f07-2a6e1b3d8c55) with reply URL https://login.acme-backup-services.com/oauth/callback; 'Add OAuth2PermissionGrant.' at 02:53:10 with ConsentType AllPrincipals and scope Mail.ReadWrite Mail.Send Mail.Read.All offline_access User.Read.All; 'Consent to application.' with IsAdminConsent True at 02:54:02.

9 STAGE

Transport rule and mailbox forwarding send finance mail outside

by **t.okafor@acme.com from 198.51.100.142**

- New-TransportRule 'Journal Archive Compliance' blind-copying internal mail containing invoice/payment/wire/remittance/bank/IBAN/swift to archive@acme-backup-services.com; Set-Mailbox on priya.raghavan@acme.com at 03:21:08 setting ForwardingSmtpAddress smtp:collect@acme-backup-services.com with DeliverToMailboxAndForward True.

10 STAGE

Permanent deletion burst in two compromised mailboxes

by **198.51.100.142**

- 61 HardDelete (permanent) events: marcus.lee 26 events 22:40:03-22:48:11 and dana.whitfield 35 events 22:40:34-22:47:59, plus 38 MoveToDeletedItems up to 22:55:30 — 99 removal events in 15 minutes.

11 STAGE

Attempt to switch off the tenant audit log (failed)

by **t.okafor@acme.com from 198.51.100.142**

- Set-AdminAuditLogConfig with UnifiedAuditLogIngestionEnabled False; ResultStatus Failed, 'InsufficientPrivileges'. The attempt failed, which is why the earlier record survives.

12 STAGE

Attacker returns and deletes its own inbox rule

by **198.51.100.142**

- Remove-InboxRule on dana.whitfield@acme.com removing the rule named '.', from the attacker address — access to the mailbox still alive four days after the OAuth grant.

13 STAGE

Defender remediation

by **elena.calderon@acme.com from 203.0.113.12**

- Password resets for dana.whitfield, marcus.lee, priya.raghavan and t.okafor (09:02-09:09); Update StsRefreshTokenValidFrom for the same four (09:20-09:22); transport rule removed (09:41); three inbox rules removed (09:50-09:52); priya.raghavan forwarding cleared (10:03); svc-backup-sync removed from role (10:18) and disabled (10:22); audit log re-enabled (11:40). No event removes the rogue OAuth application or its AllPrincipals grant.

14 STAGE

Unauthorised access continues after remediation via the OAuth application

by **198.51.100.201/.207/.213/.219/.224 as app 7b2e9a14**

- 115 events, all on priya.raghavan@acme.com, from five addresses that appear nowhere earlier in the log; 113 MailItemsAccessed (folder \Inbox\Banking among them) plus 2 Send, running to 2026-08-29T13:18:59. AuditData AppId/ClientAppId 7b2e9a14-5c83-4d16-9f07-2a6e1b3d8c55, UserType 3, ClientInfoString 'Client=REST;Client=RESTSystem;;'.

FINDINGS REGISTER

Findings (21)

Each finding cites the command that produced it. Before this report was written that command was re-run: findings that reproduced are marked Verified.

Finding 01

Mailbox compromise of dana.whitfield and immediate creation of a hiding rule

CRITICAL T1078.004 Verified — command re-run

Filtering the log to UserId dana.whitfield@acme.com AND ClientIP 198.51.100.74 shows a compact attack burst on 2026-08-03: UserLoggedIn 14:31:55, Update user. 14:38:02, New-InboxRule 14:41:19, then 420 MailItemsAccessed between 14:45:07 and 16:15:09 and 7 SearchQueryInitiatedExchange between 16:18:21 and 16:28:57. The next morning (2026-08-04) the same address sends 14 messages between 09:12:00 and 09:18:43. The account continued to be used from ordinary corporate addresses (203.0.113.x) across the same period, so the 198.51.100.74 session is an addition to normal use, not a replacement for it.

WHAT TO DO

Revoke all refresh tokens and sessions for dana.whitfield@acme.com; force a password reset. Treat her mailbox contents as disclosed: 420 item reads and 7 keyword searches of the message store.

Finding 02

Inbox rules planted to hide security alerts from four users

CRITICAL T1564.008 Verified — command re-run

Four New-InboxRule events exist in the whole log (dana.whitfield 2026-08-03T14:41:19 from 198.51.100.74; marcus.lee 2026-08-04T12:03:44; priya.raghavan 2026-08-05T08:51:17; t.okafor 2026-08-06T13:11:38 — the last three from 198.51.100.142). All four have identical Parameters: SubjectOrBodyContainsWords 'phish;suspicious;security alert;unusual sign-in;password;verify your;Microsoft account;unrecognised device;report this', MoveToFolder 'Deleted Items', MarkAsRead 'True', StopProcessingRules 'True', and ExternalAccess true. The rule names are meaningless single characters ('.', '..', ',', ';') — machine- or script-created, not user-created. The single purpose of the rule is to make phishing warnings, password-reset notices and security alerts invisible to the mailbox owner.

WHAT TO DO

Remove these four inbox rules. Alert on New-InboxRule where the rule moves mail to Deleted Items, marks it read, or stops processing. Review any rule with a non-word name.

Finding 03

Backdoor service account created and given Organization Management

CRITICAL | T1136.003, T1098.003 | Verified — command re-run

Querying the whole log for the object svc-backup-sync@acme.com returns four events. On 2026-08-06T13:19:04 t.okafor@acme.com from 198.51.100.142 ran 'Add user.' creating svc-backup-sync@acme.com (DisplayName 'Backup Sync Service', AccountEnabled true). Nine minutes later, 13:28:47, the same actor ran 'Add member to role.' adding that account to role 'Organization Management' (TemplateId 62e90394-69f5-4237-9190-012177145e10) — the most powerful Exchange/tenant admin role. The same actor then added it to a mailbox at 13:35:12 (Add-MailboxPermission). The account was only removed from the role and disabled on 2026-08-14 by elena.calderon@acme.com.

WHAT TO DO

Confirm svc-backup-sync@acme.com is not a legitimate service account. Keep it disabled, delete it, and audit every action taken by it between 2026-08-06 and 2026-08-14.

Finding 04

Malicious OAuth application granted tenant-wide mail access

CRITICAL | T1098, T1550.001 | Verified — command re-run

Three events share ObjectId 7b2e9a14-5c83-4d16-9f07-2a6e1b3d8c55, all by t.okafor@acme.com from 198.51.100.142. 2026-08-07T02:51:44 'Add service principal.' creates an app DisplayName 'ACME Mail Connector' with reply address https://login.acme-backup-services.com/oauth/callback — a look-alike domain, not acme.com. 02:53:10 'Add OAuth2PermissionGrant.' with ConsentType [AllPrincipals] and Scope 'Mail.ReadWrite Mail.Send Mail.Read.All offline_access User.Read.All' against Microsoft Graph. 02:54:02 'Consent to application.' with ConsentContext.IsAdminConsent [True]. AllPrincipals plus admin consent means every mailbox in the tenant is readable and sendable by an application under the attacker's control, independent of any user password and surviving password resets.

WHAT TO DO

Delete the service principal 7b2e9a14-5c83-4d16-9f07-2a6e1b3d8c55 and revoke its grants; block login.acme-backup-services.com. Restrict who may grant tenant-wide admin consent and alert on ConsentType AllPrincipals.

Finding 05

Transport rule silently blind-copies finance mail to an external domain

CRITICAL T1114.003 Verified — command re-run

On 2026-08-07T03:12:33 t.okafor@acme.com from 198.51.100.142 created a transport rule named 'Journal Archive Compliance' (ObjectId 'Journal Archive Compliance'). Its parameters are Name 'Journal Archive Compliance', BlindCopyTo 'archive@acme-backup-services.com', FromScope 'InOrganization', SubjectOrBodyContainsWords 'invoice;payment;wire;remittance;bank;IBAN;swift', Mode 'Enforce', Priority '0', and ExternalAccess true. The rule copies every internal message mentioning payment or banking terms to an address outside acme.com, named to look like an internal compliance control.

WHAT TO DO

Remove the 'Journal Archive Compliance' transport rule. Block archive@acme-backup-services.com. Restrict New-TransportRule to trusted admins and alert on any rule with an external BlindCopyTo.

Finding 06

priya.raghavan mailbox still read from five new addresses after the remediation

CRITICAL T1078.004 Verified — command re-run

The remediation on 2026-08-14 ran from 09:02 to 11:40 (password resets, refresh-token revocations, rule and forwarding removal, backdoor account disabled). Mailbox reading of priya.raghavan@acme.com did not stop. Filtering the log to the five source addresses 198.51.100.201, .207, .213, .219 and .224 returns 115 events, every one of them on priya.raghavan@acme.com, the earliest at 2026-08-14T18:08:26 — six and a half hours after the remediation — and the latest at 2026-08-29T13:18:59, the end of the log. 113 are MailItemsAccessed and 2 are Send operations (2026-08-19T11:26:04 from .201 and 2026-08-26T15:48:31 from .224). None of these five addresses appears anywhere in the log before 2026-08-14. Nothing in the log removed the OAuth application the attacker had created, and an AllPrincipals Mail.ReadWrite/Mail.Send grant is exactly the mechanism that survives a password reset and a token revocation, so the reading of priya.raghavan's mailbox continuing from new addresses after every credential was reset is the signature of the application grant still being alive.

WHAT TO DO

This is not remediated. Enumerate and remove every OAuth2 permission grant with ConsentType AllPrincipals in the tenant, delete service principal 7b2e9a14-5c83-4d16-9f07-2a6e1b3d8c55, and re-check priya.raghavan@acme.com after doing so. Treat her mailbox as under continuing unauthorised access.

Finding 07

Rogue OAuth application is the live access path: app 7b2e9a14 reads priya.raghavan's Banking folder over REST

CRITICAL | T1550.001 | Verified — command re-run

The MailItemsAccessed events against priya.raghavan@acme.com that fall after the remediation are not user sessions at all. Their AuditData carries AppId and ClientAppId '7b2e9a14-5c83-4d16-9f07-2a6e1b3d8c55' — the identical identifier of the application t.okafor created and consented on 2026-08-07 — with UserType 3 and ClientInfoString 'Client=REST;Client=RESTSystem;;'. The first such event, 2026-08-14T18:08:26, binds the \Sent Items folder; the one at 18:10:06 binds the folder \Inbox\Banking. A user-logon session cannot produce these rows: the recorded principal is the application, it reaches the mailbox over REST, and it survived four password resets and four refresh-token revocations performed the same morning. This is the mechanism, and it is still running at the end of the log.

WHAT TO DO

Delete service principal 7b2e9a14-5c83-4d16-9f07-2a6e1b3d8c55 and revoke its AllPrincipals grant; verify no further MailItemsAccessed carries ClientAppId of that application. Hunt for the same ClientAppId in other tenants.

Finding 08

Business email compromise: fraudulent remittance emails sent to an external supplier through the OAuth app

CRITICAL | T1114.002, T1657 | Verified — command re-run

Two Send operations in the log are attributed to priya.raghavan@acme.com with UserType 3 and AppId 7b2e9a14-5c83-4d16-9f07-2a6e1b3d8c55 — the intruder's OAuth application, not the user. 2026-08-19T11:26:04 from 198.51.100.201 and 2026-08-26T15:48:31 from 198.51.100.224, both carrying Subject 'Updated remittance details - please action' and both addressed to ap@kestrel-logistics.com, an external domain. Alongside these, the application repeatedly bound the folder \Inbox\Banking in the same mailbox (2026-08-14T18:10:06, 2026-08-15T09:21:10). Reading a folder named Banking and then sending 'updated remittance details' to an outside supplier from the finance mailbox is payment-redirection fraud, and it is the first concrete sign of what the intrusion was for. Both sends fall after the 2026-08-14 remediation, so the fraud attempt is ongoing, not historical.

WHAT TO DO

Contact kestrel-logistics.com and warn them that any payment or remittance change purporting to come from acme.com after 2026-08-19 may be fraudulent. Verify no payment was redirected, reverse any that was, and treat the two messages as evidence rather than deleting them.

Finding 09

Backdoor service account granted FullAccess to priya.raghavan's mailbox

CRITICAL T1098.002 Verified — command re-run

The log contains exactly two MailboxPermission events. At 2026-08-06T13:35:12, six minutes after t.okafor@acme.com added the backdoor account to Organization Management, the same actor from 198.51.100.142 ran Add-MailboxPermission against priya.raghavan@acme.com with Parameters User 'svc-backup-sync@acme.com', AccessRights 'FullAccess' and InheritanceType 'All'. That gave the attacker's own service account standing delegated access to the mailbox of a compromised colleague — a second, independent way to read her mail that does not involve her credentials at all. It was revoked at 2026-08-14T10:31:55 by elena.calderon@acme.com from 203.0.113.12 with the note 'delegated full access revoked'.

WHAT TO DO

Confirm no other mailbox has an unexpected FullAccess delegate; hunt for svc-backup-sync@acme.com in mailbox delegation lists across the tenant, not only in priya.raghavan's.

Finding 10

Password spray against 119 accounts from a single external address

HIGH T1110.003 Verified — command re-run

Every failed sign-in in the 46-day log comes from one source. Grouping UserLoginFailed by ClientIP returns exactly one row: 198.51.100.9, 240 events, 119 distinct UserId values, first 2026-07-27T03:11:00, last 2026-07-27T03:38:53. That is 240 attempts spread thinly over 119 accounts in 28 minutes — the shape of a password spray, not of a user mistyping. The 241st row in the log with ResultStatus=Failed is an unrelated Set-AdminAuditLogConfig by t.okafor@acme.com on 2026-08-10 (InsufficientPrivileges).

WHAT TO DO

Block 198.51.100.9 at the perimeter. Review sign-in logs for the same 119 accounts after 2026-07-27. Enable smart lockout / banned-password lists and require MFA (password alone should not be sufficient).

Finding 11

Mailbox forwarding rule set to send all mail to an external collector

HIGH T1114.003 Verified — command re-run

On 2026-08-07T03:21:08, sixty seconds after the transport rule was created, a Set-Mailbox event for priya.raghavan@acme.com ran from 198.51.100.142 with Parameters ForwardingSmtpAddress 'smtp:collect@acme-backup-services.com' and DeliverToMailboxAndForward 'True', and ExternalAccess true. A copy of every message to priya.raghavan's mailbox was therefore relayed to an external collector while her own mailbox kept working, so nothing looked broken to the user.

WHAT TO DO

Clear the forwarding address on priya.raghavan@acme.com (the log shows it was cleared on 2026-08-14). Alert on Set-Mailbox with a non-empty ForwardingSmtpAddress, and block outbound mail to acme-backup-services.com.

Finding 12

Attempt to switch off the tenant audit log, which failed

HIGH T1562.008 Verified — command re-run

The log holds exactly two Set-AdminAuditLogConfig events, and they are a matched pair. At 2026-08-10T01:15:22 t.okafor@acme.com from 198.51.100.142 attempted to set UnifiedAuditLogIngestionEnabled to False — i.e. to switch off the tenant's audit log — and the attempt FAILED with ResultStatusDetail 'InsufficientPrivileges'. At 2026-08-14T11:40:12 elena.calderon@acme.com, part of the remediation, set UnifiedAuditLogIngestionEnabled to True successfully. The attacker's attempt to blind the tenant failed, which is why this record exists at all.

WHAT TO DO

The attempt failed, but treat audit-configuration permissions as a control: alert on any Set-AdminAuditLogConfig, and verify the tenant does not rely on a role that can later be granted.

Finding 13

Permanent deletion of 61 messages from two compromised mailboxes

HIGH T1070.008 Verified — command re-run

Grouping the 61 HardDelete events by mailbox and source address returns only two rows, both from 198.51.100.142 on the night of 2026-08-09: dana.whitfield@acme.com 35 events between 22:40:34 and 22:47:59, and marcus.lee@acme.com 26 events between 22:40:03 and 22:48:11. HardDelete is permanent removal from the recoverable-items store, not an ordinary delete — an ordinary delete is SoftDelete or MoveToDeletedItems, and both of those appear elsewhere in the log from normal corporate addresses. These 61 are the only permanent deletions in the 46-day window, they are confined to the two already-compromised mailboxes, and they are confined to an eight-minute burst from the attacker's address.

WHAT TO DO

Preserve the mailboxes of dana.whitfield and marcus.lee before further retention expires. Alert on HardDelete outside an administrative change window.

Finding 14

Attacker returned on 2026-08-11 and deleted its own inbox rule

HIGH T1070.008 Verified — command re-run

The log holds exactly four Remove-InboxRule events. The first is the significant one: 2026-08-11T04:06:51, ObjectId 'dana.whitfield@acme.com\..' (the attacker's own rule), attributed to dana.whitfield@acme.com but performed from ClientIP 198.51.100.142 — the attacker's address. So the intruder still held access to dana.whitfield's mailbox on 2026-08-11, four days after creating the tenant-wide OAuth application and two days after the HardDelete burst, and used that access to delete its own hiding rule. The remaining three removals (marcus.lee 09:50:00, priya.raghavan 09:51:03, t.okafor 09:52:06 on 2026-08-14) were performed by elena.calderon@acme.com from 203.0.113.12 as part of the response.

WHAT TO DO

Treat this as proof of access persisting to 2026-08-11. Revoke and rebuild all sessions and tokens for every mailbox the attacker touched, and hunt for any further mailbox-rule or delegate changes after 2026-08-09.

Finding 15

Internal phishing launched from dana.whitfield's compromised mailbox

HIGH | T1566.002, T1078.004 | Verified — command re-run

Filtering the log to Send operations from 198.51.100.74 returns 14 messages, all attributed to dana.whitfield@acme.com, all sent between 2026-08-04T09:12:00 and 09:18:43 (one every 31 seconds, machine-like), all with Subject 'ACME Invoice Portal - Action Required' and Attachment 'Invoice_Portal_Access.html', ClientInfoString 'Client=OWA;Action=ViaProxy', items held in the \Drafts folder. The 14 recipients are marcus.lee, priya.raghavan, t.okafor, ashley.lombardi, scott.nguyen, michael.nguyen, hannah.silva, laura.bauer, gregory.kaminski, hannah.patel, mark.oconnell, eric.andersson, ronald.lombardi and timothy.silva, all @acme.com. This is the pivot. The three colleagues who were themselves compromised later — marcus.lee (first unauthorised access 2026-08-04T11:47:09, two and a half hours after the last lure), priya.raghavan (2026-08-05) and t.okafor (2026-08-06) — are all in this recipient list, and the lure was sent from a trusted internal sender so it would not be filtered. The timing places the phishing before those compromises; I cannot see from these logs whether any recipient opened the attachment.

WHAT TO DO

Warn all 14 recipients, quarantine the message 'ACME Invoice Portal - Action Required' with attachment Invoice_Portal_Access.html across the tenant, and force credential resets for any recipient who interacted with it. Treat inbound mail from compromised internal accounts as hostile.

Finding 16

Every account later compromised was itself targeted by the spray

HIGH | T1110.003 | Verified — command re-run

Filtering the 240 UserLoginFailed events on 2026-07-27 down to the four accounts that were later accessed without authorisation returns all four: dana.whitfield@acme.com 1 attempt, marcus.lee@acme.com 1, priya.raghavan@acme.com 1 and t.okafor@acme.com 3 — six failed attempts in total. Each was tried only one to three times, which is what keeps a spray under account lockout thresholds, and all four were among the 119 accounts the spray targeted. The three accounts that then took over the other three victims (t.okafor, marcus.lee, priya.raghavan) all appear here alongside the first victim. I can show the correlation between the spray target list and the set of accounts later abused; I cannot tell from these logs whether a sprayed password was reused successfully or whether the phishing lure of 2026-08-04 was the mechanism.

WHAT TO DO

Prioritise these four accounts in the credential-reuse review: check whether any password sprayed on 2026-07-27 was still valid, and confirm the lockout threshold is low enough to interrupt a one-to-three-attempt-per-account spray.

Finding 17

Exactly four interactive sign-ins from attacker addresses, one per victim

HIGH T1078.004 Verified — command re-run

The entire log contains only four UserLoggedIn events whose ClientIP falls in 198.51.100.x, and they are one per victim: dana.whitfield@acme.com from 198.51.100.74 at 2026-08-03T14:31:55, marcus.lee@acme.com from 198.51.100.74 at 2026-08-04T11:47:09, priya.raghavan@acme.com from 198.51.100.142 at 2026-08-05T08:33:26 and t.okafor@acme.com from 198.51.100.142 at 2026-08-06T13:02:51. One interactive sign-in per account on four consecutive days, with no repeat and no failures against any of them at the moment of access. This is the shape of credentials already in hand being used once to establish a session, after which the attacker worked through mailbox and API calls rather than signing in again — not of online guessing against the accounts themselves. It also fixes the earliest unauthorised access to each mailbox, which is what determines how much mail was exposed.

WHAT TO DO

Treat 2026-08-03T14:31:55, 2026-08-04T11:47:09, 2026-08-05T08:33:26 and 2026-08-06T13:02:51 as the disclosure start times for the four mailboxes when assessing the scope of exposed mail.

Finding 18

Attacker-controlled phone number registered as dana.whitfield's MFA method

HIGH T1556.006 Verified — command re-run

Only one event in the entire log sets an AltPhoneNumber. At 2026-08-03T14:38:02, seven minutes after the first unauthorised mailbox access and attributed to dana.whitfield@acme.com from 198.51.100.74, an 'Update user.' event changed the property StrongAuthenticationMethod from OldValue '[{"MethodType":3,"Default":true}]' to NewValue '[{"MethodType":1,"Default":true,"AltPhoneNumber":"+1 555 0199"}]'. In other words dana's existing default second factor was replaced with a method whose default phone number is +1 555 0199, a number chosen by whoever was at 198.51.100.74. Setting a second factor you control on an account you have taken over is how the account stays reachable after a password reset, and it is the reason the 2026-08-14 response cleared StrongAuthenticationMethod to '[]' on all four victims.

WHAT TO DO

Establish whether +1 555 0199 belongs to dana.whitfield; if not, treat it as attacker-controlled. Alert on any change to StrongAuthenticationMethod and re-enrol the four victims with methods verified in person.

Finding 19

Scope of data exposure: 861 mail items read across exactly four mailboxes

HIGH | T1114.002 | Verified — command re-run

Grouping the 861 MailItemsAccessed events that originate from 198.51.100.x by mailbox gives the exposure figure for each victim: priya.raghavan@acme.com 219, dana.whitfield@acme.com 420, t.okafor@acme.com 116, marcus.lee@acme.com 106. Those four totals sum to exactly the 861 events from attacker addresses, so no fifth mailbox was read. To this should be added 61 HardDelete and 38 SoftDelete operations (99 messages destroyed), 7 keyword searches of dana.whitfield's mailbox, and the fact that the OAuth application's Mail.Read.All grant covered every mailbox in the tenant whether or not it was exercised. In the same sweep, filtering attacker addresses by Workload returns only Exchange and AzureActiveDirectory — no SharePoint, Teams or OneDrive activity — so I can state that no file-storage content was touched from these addresses, though I cannot rule out access obtained by means not recorded here.

WHAT TO DO

Use these four figures when deciding what to disclose: 861 items were read and 99 permanently destroyed across four mailboxes. Because the AllPrincipals grant was tenant-wide, treat every mailbox as potentially exposed until the application is deleted.

Finding 20

Attacker permanently destroyed the security alerts that would have warned the users

HIGH | T1070.008, T1564.008 | Verified — command re-run

The 61 HardDelete events were not routine cleanup. Filtering them to those whose AffectedItems name a security notification leaves 50: 28 in dana.whitfield's mailbox and 22 in marcus.lee's. The subjects recorded in those events are 'Security alert: new sign-in from an unrecognised device', 'Microsoft account unusual sign-in activity', 'Suspicious activity detected on your account' and 'Your password was recently changed' — located in \\Deleted Items and destroyed permanently with HardDelete, which is removal from the recoverable-items store rather than an ordinary delete. In the same window the intruder issued 9 MoveToDeletedItems against the same class of message (marcus.lee 7, dana.whitfield 2). This is the companion to the inbox rules: where the rules prevented warnings arriving, these operations destroyed the warnings that had already arrived, so neither the users nor the service desk would see them.

WHAT TO DO

Recover what remains from the recoverable-items store and from mail-flow logs, since the alert mail is the primary record of what the users were told. Train the service desk that the absence of alert mail is not evidence the alerts did not fire.

Finding 21

Attacker activity is confined to Exchange and Azure AD, with no file-storage workload

LOW T1114 Verified — command re-run

I wanted to bound the exposure question 'was file content taken as well as mail', so I grouped every event from the 198.51.100.x range by Workload. The result is two groups and no others: Exchange 1004 and AzureActiveDirectory 250, which sum to the 1254 matched events. There is no SharePoint, OneDrive, Teams or Exchange file-workload row anywhere in the attacker-address set. On these logs the intrusion is a mail-and-directory intrusion: the 861 mailbox reads, the 121 deletion operations, the phishing and the remittance fraud are all Exchange, and every tenant-level change is Azure AD. File-storage content cannot be shown to have been touched from these addresses; that is a statement about what these logs contain, not proof that no document was ever accessed by other means.

WHAT TO DO

Scope the disclosure to mail content and directory configuration. Do not treat the absence of SharePoint activity in these logs as assurance that no document was accessed, because this bundle is an Exchange/ Azure AD audit extract.

THREAT INTELLIGENCE

Indicators

Worth blocking, and worth hunting for across the rest of your estate.

TYPE	VALUE	CONTEXT
account	svc-backup-sync@acme.com	
app_id	7b2e9a14-5c83-4d16-9f07-2a6e1b3d8c55	
domain	acme-backup-services.com	
email	ap@kestrel-logistics.com	
email_subject	ACME Invoice Portal - Action Required / Invoice_Portal_Access.html	
ip_range	198.51.100.201, 198.51.100.207, 198.51.100.213, 198.51.100.219, 198.51.100.224	
ip_range		

TYPE	VALUE	CONTEXT
	198.51.100.9, 198.51.100.74, 198.51.100.142	
phone	+1 555 0199	

DETECTION

Rules written for your data

These were written during this investigation, against the column names in your own exports. They are standard Sigma, so they can be loaded into your SIEM as they are — this is what catches the same activity next time, after this report is filed.

password-spray-ropc-many-accounts

Password spray against many accounts using ROPC authentication

HIGH | 240 matches in this evidence | attack.t1110.003

A single source address attempts non-interactive resource-owner-password-credential sign-ins against many distinct accounts in a short period. In this tenant 240 such failures hit 119 accounts from 198.51.100.9 inside 28 minutes.

SIGMA

```
title: Password spray against many accounts using ROPC authentication
id: 8b1f9c22-1a4d-4f7e-9c31-2d5b7e0a4411
status: experimental
description: >
  A single source address attempts non-interactive resource-owner-password-credential
  sign-ins against many distinct accounts in a short period. In this tenant 240
  such failures hit 119 accounts from 198.51.100.9 inside 28 minutes.
level: high
tags:
  - attack.t1110.003
  - attack.initial_access
detection:
  selection:
    Operation: 'UserLoginFailed'
    AuditData|contains: 'BAV2ROPC'
  condition: selection
falsepositives:
  - Legacy POP/IMAP or automation clients that misconfigure basic authentication
```

inbox-rule-hides-security-alerts

Inbox rule hides security and phishing notifications

CRITICAL | 4 matches in this evidence | attack.t1564.008

An inbox rule moves messages to Deleted Items, marks them read and stops further rule processing. Planted by the intruder on four mailboxes to hide warning mail about the intrusion from the mailbox owner.

SIGMA

```
title: Inbox rule hides security and phishing notifications
id: 3c7d2e51-9b64-4a10-8f22-6e1a0c9b7d05
status: experimental
description: >
  An inbox rule moves messages to Deleted Items, marks them read and stops further
  rule processing. Planted by the intruder on four mailboxes to hide warning mail
  about the intrusion from the mailbox owner.
level: critical
tags:
  - attack.t1564.008
  - attack.defense_evasion
detection:
  selection:
    Operation: 'New-InboxRule'
  hide_to_deleted:
    AuditData|contains:
      - 'Deleted Items'
  stop_processing:
    AuditData|contains:
      - 'StopProcessingRules'
  condition: selection and hide_to_deleted and stop_processing
falsepositives:
  - A user creating an aggressive bulk-mail rule by hand
```

new-account-added-to-privileged-role

Newly created account added to Organization Management

CRITICAL | 2 matches in this evidence | attack.t1136.003 | attack.t1098.003

An account is created and added to a privileged Exchange/Entra admin role within a short window. Here svc-backup-sync@acme.com was created at 13:19:04 and added to Organization Management at 13:28:47 on 2026-08-06.

SIGMA

```
title: Newly created account added to Organization Management
id: 5e9a4b73-2d18-4c60-b3a7-8f0d1e6c2a94
status: experimental
description: >
  An account is created and added to a privileged Exchange/Entra admin role within
  a short window. Here svc-backup-sync@acme.com was created at 13:19:04 and added
  to Organization Management at 13:28:47 on 2026-08-06.
level: critical
tags:
  - attack.t1136.003
  - attack.t1098.003
  - attack.persistence
detection:
  create:
    Operation: 'Add user.'
  grant:
    Operation: 'Add member to role.'
    AuditData|contains:
      - 'Organization Management'
      - '62e90394-69f5-4237-9190-012177145e10'
  condition: create or grant
falsepositives:
  - Legitimate onboarding by an administrator, which should be change-controlled
```

oauth-app-tenant-wide-admin-consent

OAuth application granted tenant-wide mail access with admin consent

CRITICAL | 3 matches in this evidence | attack.t1098 | attack.t1550.001

An application is added and then granted an AllPrincipals permission grant over Microsoft Graph mail scopes with admin consent. This survives password resets and token revocation. In this tenant app 7b2e9a14-5c83-4d16-9f07-2a6e1b3d8c55 obtained Mail.ReadWrite, Mail.Send, Mail.Read.All and User.Read.All on 2026-08-07.

SIGMA

```
title: OAuth application granted tenant-wide mail access with admin consent
id: 7a2c6f18-4e35-4d92-a6b0-1c9e5f3d8b47
status: experimental
description: >
  An application is added and then granted an AllPrincipals permission grant over
  Microsoft Graph mail scopes with admin consent. This survives password resets and
  token revocation. In this tenant app 7b2e9a14-5c83-4d16-9f07-2a6e1b3d8c55
  obtained Mail.ReadWrite, Mail.Send, Mail.Read.All and User.Read.All on 2026-08-07.
level: critical
tags:
  - attack.t1098
  - attack.t1550.001
  - attack.persistence
detection:
  grant:
    Operation: 'Add OAuth2PermissionGrant.'
    AuditData|contains:
      - 'AllPrincipals'
  consent:
    Operation: 'Consent to application.'
    AuditData|contains:
      - 'Mail.ReadWrite'
      - 'Mail.Send'
  service_principal:
    Operation: 'Add service principal.'
  condition: grant or consent or service_principal
falsepositives:
  - Approved third-party backup or archiving applications; keep an allow-list
```

application-reads-mailbox-over-rest

Mailbox items accessed by an application identity over REST

HIGH | 113 matches in this evidence | attack.t1114.002

MailItemsAccessed recorded against an application principal rather than a user session (UserType 3, REST system client). This is how the intruder's OAuth application kept reading priya.raghavan@acme.com after the 2026-08-14 remediation, including the folder \Inbox\Banking.

SIGMA

```
title: Mailbox items accessed by an application identity over REST
id: 9d4b1e60-7c28-4a53-b1e9-3f6a2d8c0e15
status: experimental
description: >
  MailItemsAccessed recorded against an application principal rather than a user
  session (UserType 3, REST system client). This is how the intruder's OAuth
  application kept reading priya.raghavan@acme.com after the 2026-08-14
  remediation, including the folder \Inbox\Banking.
level: high
tags:
  - attack.t1114.002
  - attack.collection
detection:
  selection:
    Operation: 'MailItemsAccessed'
    AuditData|contains: 'Client=REST;Client=RESTSystem;;'
  condition: selection
falsepositives:
  - Approved eDiscovery, DLP or backup services that read mail as an application
```

internal-phishing-from-compromised-mailbox

Burst of identical messages sent from one internal mailbox

HIGH | 102 matches in this evidence | attack.t1566.002

Many near-identical messages with the same subject and attachment leave a single internal mailbox in a few minutes through OWA proxy. Here dana.whitfield sent 14 'ACME Invoice Portal - Action Required' lures with Invoice_Portal_Access.html in seven minutes on 2026-08-04, three of whose recipients were compromised next.

SIGMA

```
title: Burst of identical messages sent from one internal mailbox
id: 1f6c8a04-3b71-4e28-9d05-7a2b6c1e4f93
status: experimental
description: >
  Many near-identical messages with the same subject and attachment leave a single
  internal mailbox in a few minutes through OWA proxy. Here dana.whitfield sent 14
  'ACME Invoice Portal - Action Required' lures with Invoice_Portal_Access.html in
  seven minutes on 2026-08-04, three of whose recipients were compromised next.
level: high
tags:
  - attack.t1566.002
  - attack.lateral_movement
detection:
  selection:
    Operation: 'Send'
    AuditData|contains: 'Action=ViaProxy'
  lure:
    AuditData|contains:
      - 'Invoice'
      - 'Action Required'
  condition: selection and lure
falsepositives:
  - Legitimate bulk mailings from shared or finance mailboxes; baseline the sender first
```

application-sends-mail-with-payment-lure

Mail sent by an application identity mentioning remittance or bank changes

CRITICAL | 2 matches in this evidence | attack.t1114.002

An application (not a user) sends mail whose subject concerns payment or remittance details. Here app 7b2e9a14-5c83-4d16-9f07-2a6e1b3d8c55 sent 'Updated remittance details - please action' to an external supplier on 2026-08-19 and 2026-08-26, after the remediation, from priya.raghavan@acme.com.

SIGMA

```
title: Mail sent by an application identity mentioning remittance or bank changes
id: 6b0d9e37-5a14-4c82-b7f3-2e8c1a5d9046
status: experimental
description: >
  An application (not a user) sends mail whose subject concerns payment or remittance
  details. Here app 7b2e9a14-5c83-4d16-9f07-2a6e1b3d8c55 sent 'Updated remittance
  details - please action' to an external supplier on 2026-08-19 and 2026-08-26,
  after the remediation, from priya.raghavan@acme.com.
level: critical
tags:
  - attack.t1114.002
  - attack.impact
detection:
  selection:
    Operation: 'Send'
    UserType: '3'
    AuditData|contains: 'Client=REST;Client=RESTSystem;;'
  payment:
    AuditData|contains:
      - 'remittance'
      - 'payment'
      - 'bank'
  condition: selection and payment
falsepositives:
  - Approved finance automation that mails suppliers as an application
```

mfa-method-replaced-by-unknown-number

Strong authentication method changed to a new phone number

HIGH | 1 match in this evidence | attack.t1556.006

A user's default MFA method is replaced with a phone-based method carrying a new number. Here dana.whitfield's MethodType 3 default was replaced on 2026-08-03 by a MethodType 1 entry with AltPhoneNumber +1 555 0199, from attacker address 198.51.100.74, so future challenges went to the intruder.

SIGMA

```
title: Strong authentication method changed to a new phone number
id: 2e8f5a47-6b91-4d03-a5c8-7f14b9e2c630
status: experimental
description: >
  A user's default MFA method is replaced with a phone-based method carrying a new
  number. Here dana.whitfield's MethodType 3 default was replaced on 2026-08-03 by a
  MethodType 1 entry with AltPhoneNumber +1 555 0199, from attacker address
  198.51.100.74, so future challenges went to the intruder.
level: high
tags:
  - attack.t1556.006
  - attack.persistence
detection:
  selection:
    Operation: 'Update user.'
    AuditData|contains: 'StrongAuthenticationMethod'
  new_phone:
    AuditData|contains: 'AltPhoneNumber'
  condition: selection and new_phone
falsepositives:
  - Users changing their own MFA number, which should be verified with them
```

mailbox-fullaccess-granted-to-new-account

FullAccess mailbox delegation granted to an account created the same day

HIGH | 1 match in this evidence | attack.t1098.002

Add-MailboxPermission giving FullAccess to a recently created internal account. Here svc-backup-sync@acme.com received FullAccess on priya.raghavan@acme.com at 2026-08-06T13:35:12, minutes after it was created and promoted to Organization Management by the same actor from 198.51.100.142.

SIGMA

```
title: FullAccess mailbox delegation granted to an account created the same day
id: 4a1d7c96-3e58-4b27-9f61-8c0d2a5e71b3
status: experimental
description: >
  Add-MailboxPermission giving FullAccess to a recently created internal account.
  Here svc-backup-sync@acme.com received FullAccess on priya.raghavan@acme.com at
  2026-08-06T13:35:12, minutes after it was created and promoted to Organization
  Management by the same actor from 198.51.100.142.
level: high
tags:
  - attack.t1098.002
  - attack.collection
detection:
  selection:
    Operation: 'Add-MailboxPermission'
  full_access:
    AuditData|contains: 'FullAccess'
  condition: selection and full_access
falsepositives:
  - Legitimate executive-assistant or shared-mailbox delegation, which should be change-
controlled
```

transport-rule-external-blindcopy

Transport rule blind-copies mail to an external address

CRITICAL | 1 match in this evidence | attack.t1114.003

A mail-flow rule created with BlindCopyTo pointing outside the tenant, selecting messages by finance keywords. Here 'Journal Archive Compliance' copied internal mail matching invoice/payment/wire/remittance/bank/IBAN/swift to archive@acme-backup-services.com on 2026-08-07.

SIGMA

```
title: Transport rule blind-copies mail to an external address
id: 8c3b6d15-4f92-4a07-b6e1-5d2c9a8f3407
status: experimental
description: >
  A mail-flow rule created with BlindCopyTo pointing outside the tenant, selecting
  messages by finance keywords. Here 'Journal Archive Compliance' copied internal
  mail matching invoice/payment/wire/remittance/bank/IBAN/swift to
  archive@acme-backup-services.com on 2026-08-07.
level: critical
tags:
  - attack.t1114.003
  - attack.collection
detection:
  selection:
    Operation: 'New-TransportRule'
  external_copy:
    AuditData|contains:
      - 'BlindCopyTo'
      - 'ExternalAccess\":true'
  condition: selection and external_copy
falsepositives:
  - Approved journaling or compliance archiving; these should be documented and rare
```

mailbox-forwarding-to-external-address

Mailbox forwarding configured to an external recipient

CRITICAL | 2 matches in this evidence | attack.t1114.003

ForwardingSmtpAddress is set with DeliverToMailboxAndForward, so a copy of every message leaves the tenant while the user's own mailbox still works. Set on priya.raghavan@acme.com on 2026-08-07 to smtp:collect@acme-backup-services.com.

SIGMA

```
title: Mailbox forwarding configured to an external recipient
id: 5f7a2c83-9e14-4b60-a2d8-6c0f3e7b9152
status: experimental
description: >
  ForwardingSmtpAddress is set with DeliverToMailboxAndForward, so a copy of every
  message leaves the tenant while the user's own mailbox still works. Set on
  priya.raghavan@acme.com on 2026-08-07 to smtp:collect@acme-backup-services.com.
level: critical
tags:
  - attack.t1114.003
  - attack.exfiltration
detection:
  selection:
    Operation: 'Set-Mailbox'
    AuditData|contains: 'ForwardingSmtpAddress'
  external:
    AuditData|contains:
      - 'DeliverToMailboxAndForward'
      - 'ExternalAccess\":true'
  condition: selection and external
falsepositives:
  - Legitimate auto-forwarding for staff leaving the company, which should be recorded
```

unified-audit-log-ingestion-disabled

Attempt to disable unified audit log ingestion

CRITICAL | 2 matches in this evidence | attack.t1562.008

Set-AdminAuditLogConfig with UnifiedAuditLogIngestionEnabled False is an attempt to stop the tenant recording its own audit events. Attempted by t.okafor@acme.com from 198.51.100.142 on 2026-08-10 and refused with InsufficientPrivileges.

SIGMA

```
title: Attempt to disable unified audit log ingestion
id: 2b9e4f61-7c38-4d95-8a20-1e6b5c9d3f84
status: experimental
description: >
  Set-AdminAuditLogConfig with UnifiedAuditLogIngestionEnabled False is an attempt
  to stop the tenant recording its own audit events. Attempted by t.okafor@acme.com
  from 198.51.100.142 on 2026-08-10 and refused with InsufficientPrivileges.
level: critical
tags:
  - attack.t1562.008
  - attack.defense_evasion
detection:
  selection:
    Operation: 'Set-AdminAuditLogConfig'
  disable:
    AuditData|contains: 'UnifiedAuditLogIngestionEnabled'
  condition: selection and disable
falsepositives:
  - None expected; audit logging should never be switched off in production
```

mass-permanent-mailbox-deletion

Permanent deletion of many mailbox items in a short window

HIGH | 61 matches in this evidence | attack.t1070.008

HardDelete removes items permanently rather than to Deleted Items, so it destroys evidence and mail beyond ordinary recovery. 61 HardDelete events hit dana.whitfield (35) and marcus.lee (26) on 2026-08-09 from 198.51.100.142.

SIGMA

```
title: Permanent deletion of many mailbox items in a short window
id: 7d4c8a29-6b15-4e73-9f08-2a5c1e7b603d
status: experimental
description: >
  HardDelete removes items permanently rather than to Deleted Items, so it destroys
  evidence and mail beyond ordinary recovery. 61 HardDelete events hit
  dana.whitfield (35) and marcus.lee (26) on 2026-08-09 from 198.51.100.142.
level: high
tags:
  - attack.t1070.008
  - attack.impact
detection:
  selection:
    Operation: 'HardDelete'
  condition: selection
falsepositives:
  - Retention or litigation-hold purge jobs run by an approved compliance process
```

oauth-app-registration-with-external-reply-url

Service principal registered with a reply URL outside the tenant

HIGH | 1 match in this evidence | attack.t1098.001

An application is registered whose OAuth callback points at a domain that is not the organisation's. Here 'ACME Mail Connector' used https://login.acme-backup-services.com/oauth/callback on 2026-08-07, a look-alike of the customer's own domain, before being granted tenant-wide mail access.

SIGMA

```
title: Service principal registered with a reply URL outside the tenant
id: 3a6f1d84-8b27-4c59-b0e3-9d7a2f6c1485
status: experimental
description: >
  An application is registered whose OAuth callback points at a domain that is not
  the organisation's. Here 'ACME Mail Connector' used
  https://login.acme-backup-services.com/oauth/callback on 2026-08-07, a look-alike
  of the customer's own domain, before being granted tenant-wide mail access.
level: high
tags:
  - attack.t1098.001
  - attack.persistence
detection:
  selection:
    Operation: 'Add service principal.'
  reply_url:
    AuditData|contains: 'acme-backup-services.com'
  condition: selection and reply_url
falsepositives:
  - Genuine third-party SaaS applications; maintain an allow-list of vendor domains
```

security-notification-mail-deleted-permanently

Security notification email permanently deleted or purged from a mailbox

HIGH | 50 matches in this evidence | attack.t1070.008

Deletion of mail whose subject is a security notification. This is how the intruder removed the warnings already delivered; 50 HardDelete and 9 MoveToDeletedItems events of this class hit dana.whitfield and marcus.lee on 2026-08-09 from 198.51.100.142.

SIGMA

```
title: Security notification email permanently deleted or purged from a mailbox
id: 6e2b9f04-8a71-4d38-b5c2-0f4a7e1d6938
status: experimental
description: >
  Deletion of mail whose subject is a security notification. This is how the
  intruder removed the warnings already delivered; 50 HardDelete and 9
  MoveToDeletedItems events of this class hit dana.whitfield and marcus.lee on
  2026-08-09 from 198.51.100.142.
level: high
tags:
  - attack.t1070.008
  - attack.defense_evasion
detection:
  selection:
    Operation: 'HardDelete'
  notification:
    AuditData|contains:
      - 'Security alert'
      - 'unusual sign-in'
      - 'Suspicious activity'
      - 'password was recently changed'
      - 'unrecognised device'
  condition: selection and notification
falsepositives:
  - A user emptying their own security-notification mail; rare and not normally by HardDelete
```

LIMITS OF THIS ANALYSIS

What we could not determine

A forensic report is only as complete as the logs behind it. This section says plainly where the evidence ran out.

Nothing was recorded as undetermined.

CHAIN OF EVIDENCE

Evidence examined

Every accepted file was inventoried, its shape established, and swept end to end before this report could be written — 100% coverage of the accepted evidence.

FILE	SIZE	FORMAT	STATUS
acme_unified_audit_log.csv	29.9 MB	csv	Analysed in full

Findings marked **Verified** had the command that produced them re-run, and it reproduced. Findings marked **Unverified** are published as the analysis stated them but did not reproduce on re-run, and should be confirmed by hand.

The uploaded logs and the analysis environment were destroyed when this report was produced. This document is the retained record.

`Investigation 67c436b0-d0c9-470a-9e2e-19c75be37dd9 · Instructions 2026-09-21.0009+325 · Template 2026-09-20.1 · Analysis image sha256:2380bbebb7e69dd8…`