

# BEC: MAILBOX TAKEOVER

## Incident Response Playbook Excerpt

### Phases 3 and 4: Activation, Severity, Detection, and Triage

Excerpted from Playbook PH-03 of the Galactic Incident Response Playbook Collection

Developed by the Galactic Security Research Division

This document contains two phases of the full BEC: Mailbox Takeover playbook.

# TABLE OF CONTENTS

|                                                          |            |                                                           |            |
|----------------------------------------------------------|------------|-----------------------------------------------------------|------------|
| <b>Phase 3: Activation, Categorization, and Severity</b> | <b>118</b> | <b>Phase 4: Detection, Triage, and Technical Analysis</b> | <b>121</b> |
| Quick Actions: Phase 3                                   | 118        | Quick Actions: Phase 4                                    | 121        |
| 3.1 Activation Triggers                                  | 118        | 4.1 Deconfliction with Authorized Activity                | 122        |
| 3.2 Incident Category                                    | 119        | 4.2 Indicators of Compromise and Indicators of Attack     | 122        |
| 3.3 Severity Classification                              | 119        | 4.3 Detection Queries and Log Sources                     | 123        |
| 3.4 Incident Declaration                                 | 120        | 4.4 False Positive Exclusions                             | 124        |
| 3.5 First 15–30 Minutes Checklist                        | 120        | 4.5 Scope: Iterative Updates                              | 124        |
|                                                          |            | 4.H Human Dimension Assessment                            | 125        |
|                                                          |            | 4.6 Triage Confirmation Checklist                         | 126        |
|                                                          |            | 4.7 Indicators and Detection Engineering                  | 126        |

## ABOUT THIS EXCERPT

### WHAT'S INSIDE

This excerpt covers the first hour of a business email compromise response, from the moment a mailbox takeover is suspected to the point where the IR Lead authorizes containment.

Phase 3 establishes the incident. It defines the five conditions that activate this playbook, walks through categorization and severity classification, and sets out the declaration steps that put the right people on a secure channel with an open case and an initial situation report.

Phase 4 establishes what happened. It covers ruling out authorized activity, the indicators that confirm a takeover, the log sources and queries that surface attacker activity, common false positives, and how to build and update the scope of the incident as evidence comes in. It also includes guidance on interviewing the mailbox owner, who is often the best witness available.

### HOW TO USE IT

Each phase opens with a Quick Actions box. During an active incident, start there. The numbered steps are the minimum required actions for that phase, and the sections that follow provide the detail behind each one. Responders who have already completed declaration and issued the initial SITREP can move directly to Phase 4, as noted at the bottom of the Phase 3 Quick Actions.

Keep a copy of this document somewhere accessible offline. A compromised identity may also affect access to email, shared drives, and collaboration tools, so the playbook should not depend on any of them.

To prepare your team ahead of time, load this document into Claude, ChatGPT, or the AI model your team uses and ask it to run a tabletop scenario against the Phase 3 activation triggers. Walking through the steps once before an incident shortens the time it takes to execute them during one.

### REFERENCES OUTSIDE THIS EXCERPT

This excerpt references material from other parts of the Galactic Incident Response Playbook Collection, including the CORE response framework (cited as CORE §3 and CORE §5), the Declaration Record and SITREP templates (Appendix A-1 and A-2), and related playbooks PH-01, PH-02, and PH-04. These sections are not included here. Where a step depends on one, the steps in this excerpt can still be followed using your organization's existing declaration and reporting process.

### THE FULL PLAYBOOK

The complete BEC: Mailbox Takeover playbook runs over 40 pages and continues through containment, eradication, recovery, client and correspondent communication, and post-incident review. It is one of the playbooks in Galactic's full, 2,000+ page incident response playbook, which is available to Galactic partners.

## PHASE 3 — ACTIVATION, CATEGORIZATION, AND SEVERITY

### QUICK ACTIONS — PHASE 3

1. Confirm at least one activation trigger from 3.1 is met. If uncertain, treat as confirmed and proceed.
2. Select the incident family and playbook from 3.2. If uncertain between two, select the higher severity.
3. Apply the SEV-1 Default Test per CORE §3. If two or more conditions are true, set SEV-1 — in this incident type, most confirmed takeovers qualify.
4. Declare the incident per CORE §3 — open the case, complete the Declaration Record (Appendix A-1), stand up the bridge on the out-of-band channel (mandatory here), and assign IR Lead, Scribe, and Technical Owner.
5. Call the mailbox owner by phone — never through any platform the identity reaches — and instruct them: use nothing on that account, change nothing, delete nothing, stand by for an interview.
6. Issue the Initial SITREP (Situation Report) using Appendix A-2 within 30 minutes.
7. Complete the First 15–30 Minutes Checklist in 3.5.

Experienced responders: if declaration is complete and SITREP is issued, skip to Phase 4.

Within 15 minutes: the right people are working the right problem on a channel the adversary cannot read, the incident has a declared severity, a case is open, and an initial SITREP has been issued. Declaration is not delayed to determine how long the attacker has been operating — that answer comes from Phase 4, and it is usually worse than the first estimate.

### 3.1 ACTIVATION TRIGGERS

Any one of the following activates this playbook:

- 1 An inbox rule, forwarding address, or delegate is found on an account that the account owner did not create — whether found by tooling, by an administrator, or by the owner.
- 2 An internal or external correspondent reports receiving an unusual, out-of-character, or payment-related message from a genuine company address.
- 3 An employee reports messages in their sent items they did not write, replies referencing messages they never saw, or correspondence that has gone missing.
- 4 Security tooling alerts on anomalous mailbox behavior — bulk search or read activity, mass forwarding, or rule creation following an anomalous sign-in.
- 5 An active PH-01, PH-02, or PH-04 response observes attacker operation inside a client mailbox — arrival via those playbooks' pivots.

## 3.2 INCIDENT CATEGORY

Select the family at declaration. Refine after Phase 4 triage if needed — if triage reveals a different incident type, follow the pivot point at the relevant decision point rather than recategorizing in place. If uncertain between two families, select the one with the highest potential severity.

Family selected: **PH — Phishing, Social Engineering & Business Email Compromise** This playbook: **PH-03 — BEC: Mailbox Takeover** Rationale: [INSERT 1–2 sentences — which trigger fired and why this playbook over its neighbors in 1.2]

## 3.3 SEVERITY CLASSIFICATION

The severity scale and the SEV-1 Default Test are defined in CORE §3. Apply the Default Test first; if two or more conditions are true, treat as SEV-1 until formally downgraded by the IR Lead. A confirmed takeover usually scores at least two: regulated data is likely in mailbox scope, and insurer engagement is likely whenever fraud or notification exposure is on the table.

**SEV-1 for this incident type** — any of the following:

- Attacker-sent mail has reached external correspondents — the correspondent-warning clock is running
- Regulated data (PHI, payment card data, regulated financial records) is plausibly present in the affected mailbox
- The affected account holds administrative privilege (declare SEV-1, then the ID-01/ID-02 pivot in 1.3 fires)
- Multiple mailboxes show operation by the same infrastructure — campaign indicators

Immediate actions: executive briefing within 1 hour per Phase 9.4; Legal Counsel engaged same hour for the exposure and correspondent-warning questions; Phase 6 containment begins without waiting for full reconstruction.

**SEV-2 for this incident type:**

- Takeover confirmed on a single, standard-privilege mailbox with no evidence yet of attacker-sent mail and low likelihood of regulated data in scope

Immediate actions: containment per Phase 6 begins immediately; client notification within 24 hours per CORE §9; the SEV-1 questions re-asked at every scope update.

**SEV-3 for this incident type:**

- A malicious rule was created but sign-in evidence confirms access was cut (e.g., by an earlier PH-01 containment) before any collection or sending occurred — operation attempted, not achieved

Immediate actions: complete the Phase 7.1 persistence sweep for the account the same business day; verify the no-operation conclusion against the mailbox audit log; document and close per Phase 10.

### 3.4 INCIDENT DECLARATION

When a trigger from 3.1 is confirmed, the first operator on scene declares the incident per CORE §3, completing the Declaration Record (Appendix A-1).

**Declaration authority for this incident type:** Any SOC (Security Operations Center) analyst Tier 1 or above, the IR Lead, or the vCSO [INSERT — confirm or amend per deployment]. **Incident-specific**

**declaration notes:** If arriving via pivot from PH-01, PH-02, or PH-04, do not open a new case — the existing case, timeline, and evidence log carry forward per CORE §1.5, with the playbook change recorded in the case. The bridge stands up on the out-of-band channel without exception per 2.5.

### 3.5 FIRST 15-30 MINUTES CHECKLIST

- ☐ Case opened (or carried forward from a pivot); Case ID assigned
  - ☐ Family and playbook confirmed (3.2)
  - ☐ Severity set; SEV-1 Default Test applied per CORE §3
  - ☐ Incident bridge active on out-of-band channel — mandatory in this incident type
  - ☐ IR Lead, Scribe, Technical Owner assigned
  - ☐ War room details recorded in case
  - ☐ Initial SITREP issued (Appendix A-2)
  - ☐ Mailbox owner reached by phone and instructed: touch nothing, change nothing, delete nothing, stand by
  - ☐ No response activity of any kind on platforms the affected identity reaches — confirmed with everyone on the bridge
-

## PHASE 4 — DETECTION, TRIAGE, AND TECHNICAL ANALYSIS

### QUICK ACTIONS — PHASE 4

1. Check for an authorized phishing simulation, red team exercise, or administrative rule deployment covering the affected account — see 4.1. If authorized: document, close or downgrade, update detection logic. Stop here.
2. If uncertain or confirmed unauthorized: mark status as Suspected or Confirmed and continue.
3. Enumerate every rule, forward, and delegate on the affected mailbox — read-only, remove nothing yet. Removal before evidence capture destroys the reconstruction.
4. Establish the attacker activity window: first attacker sign-in to now, from identity sign-in logs and mailbox access audit per 4.3.
5. Trace everything sent from the mailbox during the window — internal and external recipients. This list drives the correspondent-warning track.
6. Establish what was read, searched, hidden, and deleted during the window, from the mailbox audit log; recover deletions where retention allows.
7. Interview the mailbox owner by phone per 4.H — what they noticed, what's missing, what they never wrote.
8. Determine the entry vector: correlate the first attacker sign-in against phishing reports, MFA prompt activity, and endpoint telemetry per 4.3.
9. Sweep for the same attacker infrastructure across all other mailboxes — the campaign question.
10. Update the scope statement and Incident Timeline (Appendix A-3) with UTC (Coordinated Universal Time) timestamps — use 4.5 to guide what to include.
11. Watch for pivot triggers as you work: payment instructions (→ PH-02), privileged account (→ ID-01/ID-02), consent grant (→ CL-01), endpoint malware source (→ MW-03), internal credential victims (→ PH-01), regulated data exposure (→ DB-01), loss/insurer (→ LR-01). Fire each at discovery — do not finish triage first.
12. Complete every item in the Triage Confirmation Checklist (4.6). Record open items — do not skip.
13. If the incident remains Suspected after completing 4.6: close the case, document findings, update detection logic. Do not proceed.
14. Update detection rules per 4.7. Get IR Lead approval before sharing any indicators outside the team.
15. Get IR Lead authorization to move to Phase 5. Record the authorization in the case.

Experienced responders: if the Triage Confirmation Checklist is complete and IR Lead has authorized the move, skip to Phase 5.

Confirm the takeover, reconstruct the attacker's window, and identify everyone their words reached. Phase 4 does not end until the IR Lead reviews the Triage Confirmation Checklist (4.6) and authorizes the move to Phase 5. The scoping rule for this incident type: the attacker had the owner's eyes and the owner's voice — scope is everything they could read and everyone they could write to. One sequencing

note: when attacker-sent mail to external parties is found, Phase 6 containment and the correspondent-warning track start immediately and run concurrently with the rest of this triage.

#### 4.1 DECONFLICTION WITH AUTHORIZED ACTIVITY

Before investing time in investigation, confirm the suspected activity is not authorized. This is the first step — not the fourth.

- ☐ Check with the vCSO and Client Technical POC (Point of Contact) for an authorized phishing simulation or red team engagement covering the account
- ☐ Check change management and RMM/PSA records (RMM — Remote Monitoring and Management; PSA — Professional Services Automation) for administrator-deployed rules, migration jobs, or compliance journaling that can resemble takeover artifacts
- ☐ Confirm with the mailbox owner which rules, forwards, and delegates they created themselves — owners forget their own automation constantly
- ☐ Identify who can attest the activity is authorized — requires both Client Technical POC and IR Lead confirmation
- ☐ If authorized: document the rationale, close or downgrade the case, and update detection logic
- ☐ If uncertain: mark status as Suspected and continue to 4.2

#### 4.2 INDICATORS OF COMPROMISE AND INDICATORS OF ATTACK

##### IoCs — evidence of past compromise:

- Inbox rules that forward externally, or that move messages matching reply/security keywords to obscure folders or deletion — concealment rules are the takeover signature
- Sign-ins to the account from hosting providers, anonymizing services, or geography inconsistent with the owner, sustained across the window
- Sent items the owner did not write, or gaps where the audit log shows sends with no surviving sent item
- A new delegate, device, MFA method, or app password added during the window
- Bulk search or bulk read activity in the mailbox audit log inconsistent with the owner's pattern

##### IoAs — evidence of active attack in progress:

- A live session on the account from attacker infrastructure right now
- Outbound messages leaving the mailbox during the investigation — the adversary is still operating
- Replies arriving to attacker-sent threads — correspondents engaging with the adversary in real time
- The same source infrastructure authenticating against other accounts during the window

### 4.3 DETECTION QUERIES AND LOG SOURCES

For each log source below, this playbook describes what to look for and what a positive result means. Run the queries in your own tooling. Store positive results in the evidence folder linked to the case.

| Log Source                                                                                      | What to Look For                                                                                                               | Positive Result Looks Like                                                                                                                            | Store Results At                          |
|-------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|
| Mailbox configuration (read-only enumeration)                                                   | Every inbox rule, forwarding setting, and delegate on the affected mailbox, with creation timestamps                           | Any rule, forward, or delegate the owner did not create — especially external forwards and hide/delete rules                                          | Evidence folder, Case ID path per CORE §4 |
| Mailbox audit log                                                                               | Rule operations, message sends, moves, deletions, searches, and folder access across the suspected window, by actor and client | Operations attributable to attacker sessions — this log is the reconstruction backbone                                                                | Evidence folder                           |
| Identity platform sign-in logs                                                                  | All sign-ins for the account from 30 days before the first artifact to now: source, device, client application, MFA result     | The attacker access pattern that defines the activity window — first attacker sign-in is the window's start                                           | Evidence folder                           |
| Email gateway message trace                                                                     | Everything sent from the account during the window, with all recipients, internal and external                                 | The attacker-sent mail list — the input to the correspondent-warning track                                                                            | Evidence folder                           |
| Identity platform audit logs                                                                    | MFA additions, device registrations, app passwords, consent grants, delegate grants during the window                          | Persistence plants — each maps to a Phase 7.1 check, and consents fire the CL-01 pivot                                                                | Evidence folder                           |
| Deleted-item / recoverable-item stores                                                          | Messages deleted during the window                                                                                             | Recovered deletions — what the attacker tried to hide, often the replies to their own sends                                                           | Evidence folder                           |
| Endpoint security / EDR telemetry                                                               | Credential-theft indicators on the owner's device across the window                                                            | Infostealer or token-theft evidence — fire the MW-03 pivot                                                                                            | Evidence folder                           |
| If mailbox audit logging was not enabled: sign-in logs, gateway trace, and owner interview only | The same reconstruction, by triangulation                                                                                      | Record the precision loss in 4.6 — impact analysis defaults toward whole-mailbox exposure and the DB-01/Legal Counsel question is asked on that basis | Evidence folder                           |

## 4.4 FALSE POSITIVE EXCLUSIONS

The legitimate activity most likely to mimic this incident type:

- **The owner's own forgotten automation.** Users create rules and forwards and forget them — the most common benign explanation for trigger 1. The owner interview settles it; an external forward to an unrecognized address does not.
- **Administrator-deployed configuration.** Compliance journaling, migration tooling, and retention policies create rule-like and delegate-like artifacts. The change record in 4.1 settles it.
- **Shared-mailbox workflows.** Delegates and send-as patterns on genuinely shared mailboxes look like takeover artifacts. The Client Technical POC confirms the intended configuration.
- **Out-of-character mail with an in-character explanation.** A correspondent's "unusual message" report sometimes traces to the owner's real but rushed message. The owner interview plus the audit log settles authorship.
- **Authorized simulations and red team activity** — covered in 4.1; always the first check.

## 4.5 SCOPE — ITERATIVE UPDATES

Initial scoping is not final scoping. Update the scope statement every time new information changes the picture. Record each update in the Incident Timeline (Appendix A-3) with a UTC timestamp and the data source that drove the change.

The scope statement must address at all times: affected mailboxes and their identities, the attacker activity window per account, everything sent (with recipient lists), everything hidden or deleted, data types present in each affected mailbox, and the entry-vector hypothesis with confidence level.

### **Blast radius guidance — look beyond the obvious:**

The identity behind the mailbox unlocks more than mail. Explicitly evaluate chat and messaging history, shared file storage, calendars, video conferencing, and every SSO-connected application — the audit trail for each, across the same window. A takeover scoped to "the mailbox" when the identity reached the document store has been scoped wrong.

Forwarding rules are retroactively silent and prospectively total: everything matching the rule from its creation to its removal left the environment. Date the rule, and treat its full match set as exfiltrated for impact-analysis purposes.

Sweep every other mailbox for the same attacker infrastructure, rule patterns, and sending behavior — takeovers travel in campaigns, and the second mailbox is usually quieter than the first.

For the owner's personal accounts and devices: evaluate whether the entry vector ran through them, and whether attacker-sent mail or forwards reached personal addresses. Note these as scope items even where IR action is out of scope, so the Phase 4.H advisory steps can be taken. Include any pre-provisioning delegated access in the review.

## 4.H HUMAN DIMENSION ASSESSMENT

A person is at the center of this incident type — the mailbox owner, whose voice the attacker borrowed. They are also the best reconstruction witness available. Address each item below before finalizing scope.

### Employee interview

- Who conducts the interview: IR Lead or designated analyst — not the person who first discovered the incident if there is any possibility of employment implications
- Interview setting: by phone or in person — never on any platform the affected identity reaches (CORE §5)
- Tone: this is fact-gathering, not discipline. Do not imply fault. Do not make statements about employment consequences.
- Questions in scope: what they noticed and when; correspondence that seems missing or threads that "skipped"; messages or meetings they did not create; any recent phishing pages, unexpected MFA prompts, or new-device sign-ins they recall (the entry-vector question); which rules and delegates are genuinely theirs; what sensitive material lives in the mailbox — the impact-analysis seed
- Questions out of scope for the IR team: anything about employment status, policy violations, or disciplinary outcomes — those belong to HR and management

The single most consequential interview answer: **what does this mailbox contain?** The owner's inventory of sensitive correspondence — patient matters, financial records, credentials sent in mail, client confidences — sets the impact-analysis priorities and frames the Legal Counsel conversation hours before the technical reconstruction completes.

### Communication with the affected person during the incident

- Keep contact on a clean channel — their personal phone is acceptable for coordination
- Tell them what to do — use nothing on the account, change nothing, delete nothing, stand by for the MFA re-registration step in Phase 8 — and why
- Do not describe the reconstruction findings, the correspondent list, or attacker activity details
- Do not tell them what the outcome will be — for their employment or for the incident

### Personal account and device advisory

If the entry vector ran through a personal account or device, or forwards reached personal addresses, advise — do not access, investigate, or remediate:

- Change passwords on personal accounts sharing any credential with the work account, starting with email and banking
- Review connected apps, rules, and recovery methods on those accounts; enable MFA
- Preserve, don't delete — keep everything until the IR team confirms nothing further is needed
- This advice protects them and the organization — it is not an accusation

### Handoff to HR and management

The IR Lead notifies HR or management that an incident involved a specific employee. The notification is limited to: an incident occurred, the employee is cooperating, and HR or management should be available for follow-up. Employment-related decisions are owned by HR and management — never the IR team.

#### 4.6 TRIAGE CONFIRMATION CHECKLIST

Answer every item before moving to Phase 5. If an item cannot be answered, record it as an open item and continue — do not skip it.

- ☐ Is this incident confirmed or still suspected? [Confirmed / Suspected — explain]
- ☐ What is the current severity? [SEV-1 / SEV-2 / SEV-3]
- ☐ What is the attacker activity window per affected account? [First attacker sign-in to containment, UTC]
- ☐ What was sent from each affected mailbox during the window, and to whom? [Attacker-sent mail list with recipients — or Unknown with the gateway-retention gap noted]
- ☐ What was hidden, moved, or deleted, and how much is recoverable? [Status]
- ☐ What data types are present in each affected mailbox, per the owner inventory and reconstruction? [PHI / PII (Personally Identifiable Information) / financial / credentials / other — this feeds the DB-01 question]
- ☐ Did any forwarding rule operate, and what is its full match set and active period? [Treat the match set as exfiltrated]
- ☐ What is the entry-vector hypothesis and confidence? [Phish / MFA fatigue / token theft / endpoint malware / unknown — endpoint malware fires MW-03]
- ☐ Is the adversary likely still active — live session or outbound activity during triage? [Yes / No / Unknown]
- ☐ Do other mailboxes show the same infrastructure or patterns? [Campaign — Yes / No / Unknown]
- ☐ Are financial transactions at risk or already executed via attacker-sent instructions? [Yes / No / Unknown — yes fires PH-02 now]
- ☐ Was mailbox audit logging enabled across the window? [If No: impact analysis defaults toward whole-mailbox exposure; record it]
- ☐ Has any pivot trigger from 1.2/1.3 been observed without its pivot being fired? [If yes, fire it now]

If the answer to "confirmed or suspected" remains Suspected after reasonable investigation: close the case, document findings, update detection logic, and do not proceed to containment.

#### 4.7 INDICATORS AND DETECTION ENGINEERING

- ☐ New IoCs and IoAs — attacker sign-in infrastructure, rule patterns, forwarding destinations, sender behaviors — captured in a single tracker linked to the case
- ☐ Detection rules updated in SIEM, identity platform, and email platform — anomalous rule creation, external forward creation, and the campaign infrastructure — with rule IDs noted in the case record
- ☐ Indicators reviewed by IR Lead for approval before sharing outside the response team per CORE §6.4

- ☐ Approved indicators shared internally across the Partner SOC with client-identifying information removed and affected system names replaced with generic descriptors
- ☐ Countermeasure effectiveness plan created — ties to Phase 8.2

**Phase 4 terminating condition:** IR Lead reviews the completed Triage Confirmation Checklist and current scope statement, confirms severity, and authorizes the move to Phase 5. This authorization is recorded in the case. Where attacker-sent mail to external parties exists, containment and the correspondent track started at discovery — this authorization formalizes the remainder.

---