CONNECTWISE

SOC Action Report

THREAT ANALYSIS REPORT

Case: #CW-SS-BEC-772

Date: Feb 25, 2026

TRUE POSITIVE: Business Email Compromise & Data Exfiltration

Confirmed malicious activity targeting financial data and account integrity.

THREAT STATUS: MITIGATED **ACTION REQUIRED: MANUAL CLEANUP VERIFIED**

Executive Summary

Coordinated compromise has been detected across [redacted].com and [redacted].com, indicating a likely Business Email Compromise (BEC) and data exfiltration campaign. The incident began with an impossible travel authentication event between Tampa, FL, and London, UK. Shortly after, a hidden inbox rule named "Sync Errors" was created on [redacted].com to silently forward financial emails to [redacted]@gmail.com. Automated playbooks successfully severed threat actor access by disabling both accounts and revoking session tokens.

Recommendations & Actions Taken:

- ☑ **Disable Users & Revoke Sessions:** Playbook successfully invalidated refresh tokens and suspended sign-ins for both [redacted]
- ☑ **Delete Suspicious Inbox Rule:** Manually removed the "Sync Errors" forwarding rule from [redacted].com to halt data exfiltration.
- ☑ **Block External Address:** Added [redacted]@gmail.com to the global Exchange blocklist.

Attack Timeline

Impossible Travel Login Detected — Feb 24 - 14:10:00
[redacted].com successfully authenticated from London, UK (82.163.43.11)

Automated Containment Triggered — Feb 24 - 14:10:20
Account suspended and session tokens revoked for [redacted].com

Malicious Inbox Rule Created — Feb 25 - 09:15:30
"Sync Errors" forwarding rule created on compromised account [redacted].com

Manual Remediation Completed — Feb 25 - 09:45:00
Analyst [redacted] Smith removed the "Sync Errors" rule and updated the global blocklist.

Impact Assessment

Account Status	SUSPENDED (2)
Data Exfiltration Risk	MODERATE - RULE ACTIVE FOR 24H
Identity Impact	M365 Sessions invalidated

Affected Entities

Entity	Detail	Baseline IP
[redacted].com	Sales Director	73.120.45.12
[redacted].com	Finance Manager	73.120.45.88

Context Hub

Context Hub

SECONDARY ENRICHMENT

Network & Threat Intel

- **82.163.43.11 (London, UK):** Resolved to a commercial anonymous VPN provider. Not a registered Salty Soul corporate egress node.
- **185.104.184.12 (Netherlands):** Flagged by Threat Intelligence as a known proxy node associated with previous credential stuffing campaigns.

SaaS & Identity Environment (ASIO)

- [redacted]**com:** The London authentication successfully bypassed MFA via a stolen session cookie (Session ID matches the earlier Tampa login).
- [redacted]**gmail.com:** Domain (gmail.com) is a free mail provider. This address has zero historical communication with any Salty Soul employee.

JIT BASELINE INDICATORS

Profile: [redacted].com)

Standard Baseline: 100% of historical logins over the past 90 days originate from Florida, USA.

Active Conflict: Concurrent geographic distance conflict detected. Authentication from Tampa, FL and London, UK occurred within a 10-minute window (requires travel speed of ~25,000 mph).

Profile: [redacted].com)

Standard Baseline: Administrative Exchange actions (rule creation/delegation) are exceedingly rare for this finance user (0 events in past 365 days).

Active Conflict: "Sync Errors" forwarding rule created from a non-standard geographic location (Netherlands) to an external, never-before-seen free email address.

MUSE TOOL USAGE RISK

Status: Not Applicable

AI Note: *No dual-use administrative tools, RMM agents (e.g., AnyDesk, TeamViewer), or localized command-line utilities (e.g., PowerShell, OSQuery) were detected in this cloud-centric attack chain.*

Detailed Threat Analysis Log

M365 Identity Login from Impossible Travel Location

2026-02-24T14:10:00Z

[redacted].com successfully authenticated from an anomalous IP in London, UK immediately after a standard baseline login from Tampa, FL.

FULL EVENT LOGS

@timestamp	event.action	o365.audit.UserId	source.ip	source.geo.country	o365.audit.ApplicationId
2026-02-24T14:00:00.000Z	UserLoggedIn	[redacted].com	73.120.45.12	United States (US-FL)	1b730954-1685-4b74...
2026-02-24T14:10:00.000Z	UserLoggedIn	[redacted].com	82.163.43.11	United Kingdom (GB-ENG)	1b730954-1685-4b74...

M365 Exchange Inbox Forwarding Rule Created

2026-02-25T09:15:30Z

A hidden inbox rule named "Sync Errors" was created on [redacted].com from a Netherlands IP address (185.104.184.12) to forward data externally.

FULL EVENT LOG

Field	Value
@timestamp	2026-02-25T09:15:30.000Z
event.provider	Exchange
event.action	New-InboxRule
o365.audit.UserId	[redacted].com
source.ip	185.104.184.12
o365.audit.Parameters.Name	"Sync Errors"
o365.audit.Parameters.ForwardTo	[redacted]@gmail.com
o365.audit.Parameters.StopProcessingRules	True

Technical Details & Analysis

Indicators of Compromise (IOCs)

```
Network (Malicious): 82.163.43.11 (London VPN)
Network (Malicious): 185.104.184.12 (Netherlands Proxy)
Email (Malicious): [redacted]@gmail.com (Drop Address)
Artifact (Persistence): InboxRule: "Sync Errors"
```

MITRE ATT&CK® Mapping

Tactic	Technique	Sub-Technique	Severity
Initial Access (TA0001)	Valid Accounts (T1078)	Cloud Accounts (T1078.004)	MEDIUM
Collection (TA0009)	Email Collection (T1114)	Email Forwarding Rule (T1114.003)	MEDIUM

Mitigation Actions

- [x] M365 Account sign-ins suspended.
- [x] Malicious Exchange rule "Sync Errors" purged.
- [x] Global blocklist updated for attacker drop address.

Analyst Notes

"Confirmed with [redacted] no travel. Automated containment verified. Manual Exchange cleanup performed on [redacted]'s mailbox to neutralize BEC data collection. Recommending hardware token resets for both users."

- [redacted] Smith, Senior SOC Analyst

Download Report as PDF