Report Date: March 15, 2025
Report ID: CM-2025-3319-28940
Classification: SAMPLE DOCUMENT

COMPROMISE ASSESSMENT REPORT

Acme Corporation (Sample Client)

Security Investigation — Business Email Compromise Incident

SAMPLE DOCUMENT — FOR DEMONSTRATION PURPOSES ONLY

259	15	HIGH	$1.2M
EVENTS ANALYZED	CRITICAL FINDINGS	OVERALL RISK LEVEL	LOSS PREVENTED

01 EXECUTIVE SUMMARY

Leadership Overview — March 15, 2025

Assessment Overview Intrusent Technologies conducted a comprehensive compromise assessment of Acme Corporation's IT infrastructure following suspicious email activity detected by their security operations team. The assessment examined email systems, endpoint devices, network traffic, and authentication logs across a 90-day lookback period spanning December 15, 2024 through March 15, 2025.

KEY FINDINGS SUMMARY

Our investigation identified evidence of a sophisticated Business Email Compromise (BEC) attack targeting the finance department, along with several security vulnerabilities requiring immediate attention. Threat actor activity was limited to email account compromise — no evidence of lateral movement, persistent access mechanisms, or data exfiltration beyond the initially compromised mailbox was observed.

Critical Findings Summary

HIGH	**Active BEC Campaign Identified** Evidence of ongoing business email compromise targeting CFO and IT team with fraudulent wire transfer requests totaling $1.2M in attempted theft (prevented by client verification controls).
MEDIUM	**Compromised Executive Email Account** Finance Director's Office 365 account (jsmith@acme-corp.com) showed unauthorized access from IP addresses geolocated to Eastern Europe (suspected VPN usage).
MEDIUM	**Privileged Account Vulnerabilities** 23 administrative accounts identified with passwords unchanged for 180+ days, including 4 domain admin accounts without MFA enabled.
ACCEPTABLE	**Effective Detection Controls** Client security team successfully identified and contained the initial compromise within 48 hours of attack initiation, preventing financial loss.
NEW	**No Lateral Movement Detected** Investigation found no evidence of threat actor movement beyond the initially compromised email account. No malware, backdoors, or persistence access mechanisms identified.

02 ASSESSMENT SCOPE & METHODOLOGY

Investigation Parameters — 90-Day Lookback

Systems Analyzed

- O365 Unified Audit Logs (Exchange, SharePoint, OneDrive)
- Microsoft Entra ID (Azure AD) sign-in logs
- Microsoft Defender for Endpoint alert history
- Network firewall logs (Palo Alto PA-5220)
- Domain controller authentication logs
- Email Security Gateway (Proofpoint TAP)
- Endpoint Detection & Response (CrowdStrike Falcon)
- Mobile Device Management (Intune)
- Privileged Access Management (CyberArk)

Email Investigation

- 15,247 email messages reviewed
- Executive mailbox deep analysis (5 users)
- External sender reputation
- Attachment detonation analysis
- URL reputation and click tracking
- Mail flow rule audit

Forensic Tools Deployed

- Magnet AXIOM Cyber v10
- Microsoft Defender for Endpoint
- Microsoft Sentinel (analysis workspace)
- Splunk Enterprise (log analysis)
- Custom YARA/Sigma rules

03 ATTACK TIMELINE RECONSTRUCTION

Timeline of Events — March 15, 2025

March 1, 2025 — 08:47 UTC

Initial Phishing Email Received
Finance Director (jsmith@acme-corp.example) receives spear-phishing email from spoofed domain (supplier-payment@acme-corp.com) — lookalike of legitimate vendor. Email contained credential harvesting link masquerading as DocuSign document.

Message ID: <20250301084712.a1b2c3d4>@acme-corp.com

March 1, 2025 — 09:12 UTC

Credential Harvesting Successful
User clicked link and entered credentials on attacker-controlled page hosted at hxxps://credential-harvest.[example]/verify. Azure AD logs show successful authentication from Tor exit IP 5.188.86.114.

Attacker IP: 185.56.[redacted]
ASN: [redacted]
Geolocation: Eastern Europe

March 1–7, 2025

Reconnaissance & Collection Phase
Threat actor conducted email reconnaissance over 5 day period. Downloaded contact lists, reviewed vendor correspondence, and studied payment procedures. Created inbox rule to auto-delete security notifications containing "alert", "security", or "breach" to external address.

Forwarding rule target: noflo.dropboxmail[redacted]

March 8, 2025 — 14:23 UTC

Fraudulent Wire Transfer Request Sent
First fraudulent wire transfer request ($847,000) sent to CFO from compromised Finance Director account. Email referenced legitimate pending vendor invoice with modified banking details.

March 8, 2025 — 16:45 UTC

BEC Detection — Anomalous Login Alert
Microsoft Defender for Cloud Apps triggered "Impossible travel" alert. SOC analyst escalated after confirming user was on site (Brooklyn) while login originated from Eastern Europe.

March 8, 2025 — 18:15 UTC

Containment Achieved
Account disabled, password reset, MFA enforced. Malicious rule found and removed. CFO verification call prevented wire transfer. Second request ($380,000) identified and blocked.

04 INDICATORS OF COMPROMISE

Threat Intelligence IC Tracker Including IP Addresses

NETWORK & INFRASTRUCTURE IOCS

TYPE	INDICATOR	CONTEXT	CONFIDENCE
IPv4	185.56.[redacted]	Attacker infrastructure (Eastern Europe)	HIGH
IPv4	185.6.131.47	Secondary login source (Eastern Europe)	HIGH
Domain	supplier-payment[redacted]	Typosquat domain (supplier0 + phishing-origin)	HIGH
Domain	credential-harvest.[redacted]	Credential harvesting page	HIGH
Email	noflo.dropboxmail[redacted]	Exfiltration email (mass rule forward target)	HIGH
URL	hxxps://credential-harvest.[redacted]/verify/MzYwNA	Credential harvesting landing page	HIGH

BEHAVIOR IOCS (MITRE ATT&CK® AUTHENTICATION EVENT)

```
2025-03-08T18:45:12Z | EnterpriseSecurity
UserPrincipalName: jsmith@acme-corp.onmicrosoft
AuthenticationMethod: Password
ClientIP: 185.56.[redacted]
ClientAppUsed: Browser
UserAgent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AuthenticationResult: Success
Location: Brooklyn, US
Risk: HighRisk
RiskEventTypes: unfamiliarFeatures
ConditionalAccessStatus: notApplied
CorrelationId: [illegible]
```

Attacker Email Inbox Rule (Microsoft 365 Defender)

```
2025-03-08T19:02:33Z | New-InboxRule
Mailbox: jsmith@acme-corp.onmicrosoft.com
ObjectId: 1ab2c3d4-5e6f-7g8h-9i0j-k1l2m3n4o5p6
Name: Security Notifications
Enabled: True
ForwardTo: noflo.dropboxmail[redacted]
DeleteMessage: True
SubjectContainsWords: "alert", "security", "breach"
MoveToFolder: "RSS Feeds"
StopProcessingRules: True
ExternalOrganizationAuditId: [illegible]
ClientIP: 185.56.[redacted]
ClientApplication: Microsoft.Exchange.ClientAccessServer
CorrelationId: [illegible]
```

Azure Sign-in Log — Impossible Travel Detection

```
2025-03-08T16:45:12Z | Azure ActiveDirectory
UserPrincipalName: jsmith@acme-corp.onmicrosoft.com
AuthenticationMethod: Password
ClientIP: 185.56.[redacted]
Location: Brooklyn, US
Risk: HighRisk
RiskEventTypes: unfamiliarFeatures
Device: "", "Firefox" per-user "Windows Home"
Prior_Locations_Last_30_Days: "Brooklyn, US", "Queens, US"
Impossible_Travel_Distance_Km: 7,412
Impossible_Travel_Time_Hours: 1.2
ConditionalAccessStatus: notApplied
CorrelationId: [illegible]
```

05 MITRE ATT&CK MAPPING

Tactics, Techniques, Procedures

Initial Access

T1566.001	**Phishing: Spearphishing Link** Targeted email to Finance Director containing link to credential harvesting page (credential-harvest.[example]). Email originated from typosquat domain impersonating known vendor.

Credential Access

T1556.006	**Modify Authentication Process: Multi-Factor Authentication** MFA not enforced on compromised account. Attacker authenticated with stolen credentials only. No MFA challenge triggered.

Collection

T1114.003	**Email Collection: Remote Email Collection** Threat actor reviewed 5 days of email over 7 days. Downloaded contact lists, reviewed financial vendor communications, and identified payment procedures.
T1114.001	**Email Collection: Email Forwarding Rule** Created hidden inbox rule (Name: "") to auto-forward emails containing financial keywords to attacker-controlled Proton Mail address.

Impact

T1657	**Financial Theft** Attempted $1.2M in fraudulent wire transfers via BEC. Two requests sent: $847K (vendor invoice modification) and $380K (urgent payment request). Both detected by financial controls.

Techniques NOT Observed

The following Tactic and Technique were specifically hunted for and NOT detected during this assessment:

TA0001 — Command & Scripting Interpreter	T1055 — Remote Services (Lateral Movement)
TA0011 — Boot/Logon Autostart (Persistence)	T1005 — Collection Over C2 Channel

06 EVIDENCE INVENTORY

Forensic Artifacts Collected

EVIDENCE ID	DESCRIPTION	SOURCE	COLLECTION DATE	SHA-256 HASH
EV-001	Azure AD Sign-in Logs (90 days)	Microsoft 365 Admin Center	2025-03-18	a8f5b6c4d3...
EV-002	Unified Audit Log (Exchange)	Office 365 Security & Compliance	2025-03-18	9d4e7f2a1b...
EV-003	Finance Director Mailbox Export (.pst)	Exchange Online eDiscovery	2025-03-18	c2b8a9d7e4...
EV-004	Phishing Email Original (.eml)	Message Trace	2025-03-18	3a1b5c9d7e...
EV-005	Cisco ASA Firewall Logs	Syslog Server	2025-03-19	7f2e4a8b1c...
EV-006	Domain Controller Security Logs	DC01, DC02 (Event Log)	2025-03-19	4b6c8d2e9f...
EV-007	Endpoint Triage Package (Finance Director PC)	Velociraptor Collection	2025-03-19	e5d1a7b3c8...

Chain of Custody Statement

All evidence was collected using forensically sound methodologies. Hash values were computed at time of collection and verified prior to analysis. Evidence packages are stored in encrypted archive with access logging enabled. Full chain of custody documentation available upon request for legal proceedings.

07 RECOMMENDATIONS

Prioritized Remediation Actions

IMMEDIATE ACTIONS (0–48 HOURS)

IMMEDIATE — CRITICAL

Enforce MFA on All User Accounts
Enable Multi-Factor Authentication for all Microsoft 365 accounts, prioritizing executives, finance, and accounts payable teams. Use phishing-resistant methods (FIDO2 keys, Windows Hello for Business) where feasible. Disable legacy authentication protocols that bypass MFA.

IMMEDIATE — CRITICAL

Audit All Mail Flow Rules Organization Wide
Review inbox rules across all mailboxes for unauthorized forwarding. Pay special attention to rules with single-character names (used to hide malicious rules). Implement alerting on new forwarding rule creation.

IMMEDIATE — HIGH

Block Identified IOCs at Perimeter
Add all IOCs from Section 04 to firewall block lists, email gateway deny lists, and DNS sinkholes. Monitor for any connection attempts to indicators to persistent compromise assess.

SHORT TERM ACTIONS (1–6 WEEKS)

SHORT TERM — HIGH

BEC-Focused Security Awareness Training
Conduct targeted training for finance and executive teams on BEC attack patterns. Include wire transfer verification procedures, domain spoofing detection (lookalike characters), and reporting suspicious requests. Follow up with simulated BEC exercises.

SHORT TERM — MEDIUM

Privileged Access Management Implementation
Deploy PAM solution with just-in-time access for administrative accounts. Enforce password rotation policy (90-day maximum) for all privileged accounts. Implement session recording for high-risk activities.

SHORT TERM — MEDIUM

External Email Warning
Implement visual indicators for all emails originating outside the organization. Consider X-header insertion for automated filtering and enhanced warning banners for first-time external senders.

STRATEGIC RECOMMENDATIONS (3–9 MONTHS)

STRATEGIC

Zero Trust Architecture Roadmap
Develop implementation plan for zero trust principles. Start with identity verification (Conditional Access policies requiring compliant devices, trusted locations). Progress to network segmentation and application-level access controls.

STRATEGIC

Continuous Threat Monitoring Enhancement
Deploy User and Entity Behavior Analytics (UEBA) for early warning of manufacturing-sector compromise. Deploy automated IOC ingestion and correlation with SIEM. Establish threat hunting cadence (monthly).

08 BUSINESS IMPACT & RISK ASSESSMENT

Strategic Analysis

Overall Security Maturity: Acme Corporation demonstrates a **Medium** security posture with effective detection capabilities but opportunities for improvement in preventative controls.

Risk Level: The identified BEC attack represents a High business risk given the potential financial impact ($1.2M+ attempted theft), but mitigation controls prevented any material loss. Reputational impact would be significant if customers were affected.

Industry Context: Based on DREAD threat intelligence, manufacturing companies are experiencing a 340% increase in BEC attacks targeting supply chain and finance processes in Q1 2025. Acme Corp's exposure is consistent with broader sector trends.

Business Impact Analysis

Worst Case	Most Likely	Best Case
Successful wire transfer fraud (prevented in this case). Potential loss of existing financial relationships and reputational damage. Regulatory notification requirements if customer data accessed.	Compromised executive email account requires extended review, credential rotation, and enhanced monitoring. Business disruption limited to 1–2 days.	Phishing attempt blocked by existing controls. Security team identifies and remediates within 24 hours. No customer impact.

Implementation Roadmap

Week 1	Deploy MFA to all privileged accounts. Complete mail flow rule audit. Block all identified IOCs.
Week 2–4	Conduct BEC awareness training for finance/executive teams. Implement external email tagging. Deploy enhanced alerting on authentication anomalies.
Month 2	Deploy PAM solution. Establish quarterly threat hunting cadence. Implement Conditional Access policies.
Month 3	Implement continuous monitoring enhancements. Conduct follow-up assessment to validate remediation. Begin zero trust planning.
Ongoing	Quarterly security posture reviews. Annual comprehensive assessments. Monthly threat hunting exercises.

Next Steps & Support

Intrusent Technologies recommends implementing critical recommendations within 48 hours. Our team is available for implementation support, quarterly security reviews, and IOC Feed updates.

EMERGENCY SUPPORT	CONTACT EMAIL	FOLLOW-UP ASSESSMENT
800 555 0820	contact@intrusent.com	90 Days Recommended

Ready for Your Own Assessment?

This sample report demonstrates Intrusent's approach to compromise assessment. Our team conducts thorough investigations to identify whether threat actors have gained access to your environment, how they got in, how deep they went, and what actions they've taken.

What You Get

- Complete forensic analysis of your environment
- Timeline of threat actor activity
- Detailed findings with severity ratings
- Actionable remediation recommendations
- Executive summary for leadership

Schedule a consultation to discuss your organization's needs.

PHONE
540 832 0820

EMAIL
contact@intrusent.com

intrusent.com/compromise-assessment

SAMPLE DOCUMENT — This report is for demonstration purposes only. All indicators, entities, and details are fictitious.

© 2025 Intrusent Technologies LLC | Orange County, California | www.intrusent.com

Report prepared by certified incident response professionals with 20+ years of cybersecurity investigation experience.