**AiTM Phishing, Credential Replay and BEC Activity – DataHaven Solutions** 2025-10-28

Title: AiTM Phishing, Credential Replay and BEC Activity – DataHaven Solutions
Date: 2025-10-28
Alert Type/Category: Successful Account Compromise / Business Email Compromise (AiTM)
Severity: High
Analyst Name:
Case #: ALRT-2025-10-27-AITM-003

# DETECTION AND ANALYSIS

## Alert Summary:

The organisation's email security controls detected delivery of a spoofed Microsoft 365-themed phishing email from support@micr0soft.com to user erik.nilsen@datahaven.no on workstation WIN10-DH-045, and correlated web proxy, DNS, identity and endpoint telemetry show that this led to a successful Adversary-in-the-Middle (AiTM) phishing attack, credential/session theft, and subsequent business email compromise (BEC) activity against the user's mailbox. The phishing message contained a link to `https://i9152.cisele0.com/NOZcbtTxxEiGj/`, where DNS and passive DNS records show `i9152.cisele0.com` resolving to 85.214.12.99 and 89.185.80.19 with a recently registered domain and a Let's Encrypt certificate, characteristics typical of AiTM phishing infrastructure that reverse-proxies Microsoft 365 login pages to intercept credentials and session cookies while presenting a legitimate-looking experience to the victim [1]. Shortly after the email was delivered, the user clicked the link, resulting in HTTP and WebSocket connections from internal client IP 10.4.23.87 to `i9152.cisele0.com`, followed by a credential POST to `/submit_login` and then successful interactive sign-ins for `erik.nilsen@datahaven.no` from external IP 89.185.80.19 using the non-browser user agent `Axios/1.7.9`, with authentication logs explicitly flagging that MFA was circumvented via an AiTM proxy and that the session was later reused via `grant_type=refresh_token`, which is consistent with known AiTM cookie-theft and token replay techniques against Microsoft 365 [1]. Using this stolen session, the attacker accessed the mailbox from the same external IP and Graph API client, executing a `GET https://graph.microsoft.com/v1.0/me/messages?$filter=contains(subject,'Invoice')` query and triggering `MailItemsAccessed` events for at least seven messages with "Invoice" in the subject, indicating that existing finance-related threads and associated invoice/payment data were opened by the adversary. Within this session, the attacker then created a mailbox rule named `_finance-forward` configured to forward messages to `attacker-relay@outlook.com` and sent an outbound email from the compromised account to `finance@victimcorp.no` with the subject "Re: Invoice Payment - Urgent" and a PDF attachment containing payment instructions, aligning with documented BEC tradecraft where attackers hijack live conversations and use mailbox forwarding rules for persistence, covert monitoring and data exfiltration [2][3]. Parallel endpoint telemetry on WIN10-DH-045 reports an EDR alert for suspicious token access patterns in the browser context tied to 89.185.80.19 and a high-risk event for a remote PowerShell-based download and execution originating from the browser session (process `powershell.exe ...`), suggesting an attempt to pivot from the cloud account into the endpoint to gain a more durable foothold. Taken together, the evidence strongly supports the hypothesis that the account `erik.nilsen@datahaven.no` has been successfully compromised via an AiTM phishing kit, that the adversary has already abused the mailbox for financial fraud and persistence, and that there are

indications of attempted endpoint compromise; we recommend that you investigate this activity further, as the activity appears to be an active and high-risk identity and email compromise.

### References:

[1] Microsoft Security Blog – “Detecting and mitigating a multi-stage AiTM phishing and BEC campaign” / “From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to further financial fraud”.
[2] MITRE ATT&CK – T1114.003 “Email Forwarding Rule” and Microsoft/XDR guidance on suspicious email forwarding activity.
[3] Palo Alto Networks & related BEC guidance – overviews of Business Email Compromise campaigns leveraging hijacked mailboxes and finance-themed threads.

## Key Details:

Customer: DataHaven Solutions

User (Identity): erik.nilsen@datahaven.no

User (Endpoint Logon): erik.nilsen

Host: WIN10-DH-045

Internal Client IP: 10.4.23.87

External Attacker IPs:
- 89.185.80.19 (AiTM proxy / attacker sign-in and Graph API activity)
- 85.214.12.99 (passive DNS for i9152.cisele0.com)

Target Cloud Service IP: 52.96.0.0 (portal.office.com A record)

Phishing Sender Address: support@micr0soft.com

Phishing Recipient Address: erik.nilsen@datahaven.no

Phishing Email Subject: Action required: Verify your account

Phishing URL: https://i9152.cisele0.com/NOZcbtTxxEiGj/

Attacker Domain: i9152.cisele0.com

Domain Registration/Cert: Newly registered domain with Let’s Encrypt certificate; seen from 2025-10-20 to 2025-10-28 (PDNS/WHOIS telemetry)

Authentication Events (Legitimate User):
- Event ID: 4624 (interactive logon to WIN10-DH-045 from 10.4.23.87, NO, Oslo)

Authentication Events (Attacker / AiTM):
- Successful interactive sign-in for erik.nilsen@datahaven.no from 89.185.80.19; location: US, Arizona; User-Agent: Axios/1.7.9; MFA circumvented via AiTM proxy
- Authentication success with session reuse / token replay for erik.nilsen@datahaven.no; grant_type=refresh_token; conditional_access=not_evaluated

Browser / Proxy Activity:
- HTTP/HTTPS requests from 10.4.23.87 to i9152.cisele0.com over TLS with WebSocket upgrade (`/socket`), long-lived WSS frames to 89.185.80.19
- HTTP 302 redirection from i9152.cisele0.com to login.microsoftonline.com as part of proxied OAuth flow

Credential Capture Indicator:
- POST https://i9152.cisele0.com/submit_login (username=erik.nilsen, password=**; redacted in logs)

Microsoft Graph API Usage (Attacker):
- Request: GET https://graph.microsoft.com/v1.0/me/messages?$filter=contains(subject,'Invoice')
- MailItemsAccessed: 7 messages with subject containing "Invoice"; client=GraphAPI; risk=high

Mailbox Rule Manipulation:
- Rule Name: _finance-forward
- Rule Action: ForwardTo attacker-relay@outlook.com
- Rule Status: Enabled=true

BEC Outbound Email:
- From: erik.nilsen@datahaven.no
- To: finance@victimcorp.no
- Subject: Re: Invoice Payment - Urgent
- Attachment(s): invoice_payment_datahaven_oct25.pdf / payment_request_80295.pdf (payment details redacted in telemetry)

UEBA Indicators:
- Anomaly: Unusual mailbox activity and outbound email to new external finance contact; risk_score=0.92; correlated with AuthService, M365 Audit and EmailGateway events

Endpoint / EDR Indicators:
- Alert Name: EDR: Suspicious Remote Download and Execution
- Host: WIN10-DH-045
- User: erik.nilsen
- Process: powershell.exe … (remote download from attacker-controlled infrastructure noted in alert metadata)
- Additional Alert: suspicious token access pattern in browser context; possible session replay/proxied credentials

Geolocation Context:
- Normal user activity: NO, Oslo
- Suspicious sign-ins, Graph API access, mailbox rule changes and BEC email: US, Arizona (external IP 89.185.80.19)

IOC Summary:
- IPs: 89.185.80.19, 85.214.12.99, 52.96.0.0 (service)
- Domain: i9152.cisele0.com
- User Agent: Axios/1.7.9

## Consequence:

This incident represents a confirmed cloud identity compromise of the account `erik.nilsen@datahaven.no` with active misuse of the associated mailbox and indications of attempted endpoint compromise. By stealing and replaying the user's session via AiTM infrastructure, the attacker gained full access to the Microsoft 365 account despite MFA, enabling them to search and open at least seven invoice-related email threads and thereby expose financial and potentially commercially sensitive information contained in those conversations and attachments. The creation of the `_finance-forward` mailbox rule forwarding email to `attacker-relay@outlook.com` provides the adversary with ongoing visibility into future correspondence, supports continued data exfiltration of finance-related messages, and offers a persistence mechanism that can survive initial remediation steps if not fully removed, matching known post-compromise techniques for collection and covert monitoring [2]. The outbound BEC email to `finance@victimcorp.no` with modified payment instructions demonstrates that the attacker has already weaponised the compromise to attempt financial fraud against an external party, which may lead to direct monetary loss if the request is actioned. In addition, the suspicious browser token-access alerts and the EDR detection for a remote PowerShell download indicate an effort to extend the intrusion from the cloud account into the endpoint (WIN10-DH-045), which, if successful, could allow the attacker to deploy additional malware, harvest local credentials, pivot deeper into the internal network, and potentially impact other systems and data beyond the initial mailbox and cloud identity.

# CONTAINMENT

## Executed Remediation Actions:

The following containment and eradication actions has been performed by our SOC:
- No actions applicable by the MDR SOC due to customer contract.

## Recommended Remediation Actions:

Our SOC recommends that you do the following containment actions:
- Immediately disable or lock the user account `erik.nilsen` / `erik.nilsen@datahaven.no` in Active Directory / Entra ID and block further sign-ins until the incident has been fully contained.
- Force a global sign-out and revoke all active refresh tokens and session cookies for the compromised account, then reset the password and require re-enrolment of MFA on trusted devices only.
- Remove the `_finance-forward` mailbox rule and any other suspicious rules from the user's mailbox, and temporarily block automatic forwarding to external addresses such as `attacker-relay@outlook.com`.
- Block outbound connections to the attacker infrastructure (IPs 89.185.80.19 and 85.214.12.99 and domain `i9152.cisele0.com`) on email gateways, web proxies, firewalls and other relevant perimeter controls.
- Run a full antivirus/EDR scan of WIN10-DH-045; if any additional malicious artefacts or scripts are detected, reimage the endpoint from a known-good baseline and re-onboard it to the EDR platform before returning it to production.
- Review Microsoft 365 sign-in, audit and MailItemsAccessed logs for additional access from

89.185.80.19 / 85.214.12.99 or the `Axios/1.7.9` user agent, and apply the same account-disable, token revocation and mailbox rule clean-up steps to any other affected users.
- Contact the external recipient `finance@victimcorp.no` through an out-of-band channel to warn them about the fraudulent “Re: Invoice Payment - Urgent” email and confirm that no payments have been or will be processed based on those instructions, following your internal fraud response process.