Title: AiTM phishing leading to account compromise and BEC (DataHaven Solutions)
Date: 2025-10-28
Alert Type/Category: Adversary-in-the-Middle (AiTM) phishing and account compromise
Severity: High
Analyst Name:
Case #: ALRT-2025-10-27-AITM-003

DETECTION AND ANALYSIS

Alert Summary:

Email gateway, web proxy, identity, and endpoint telemetry detected a successful Adversary-in-the-Middle phishing flow impacting user erik.nilsen@datahaven.no on host WIN10-DH-045. The campaign spoofed Microsoft with urgency (“Action required: Verify your account”) and directed the user to https://i9152.cisele0[.]com/NOZcbtTxxEiGj/, a Tycoon AiTM kit domain [1], where a captcha and heavily obfuscated script (myscr81234.js) loaded in Edge, followed by a long-lived WebSocket to the same domain (resolving to 85.214.12.99 and observed via 89.185.80.19). After credential submission through the proxy, an OAuth token was issued for the user, and within seconds a successful non-browser login using Axios/1.7.9 from 89.185.80.19 replayed the session to Microsoft Graph, accessing mailbox items and creating a forwarding rule (“_finance-forward” to attacker-relay@outlook.com). The compromised mailbox then sent an outbound BEC email (”Re: Invoice Payment – Urgent”) to finance@victimcorp.no with updated payment instructions. EDR simultaneously flagged suspicious remote activity including PowerShell execution tied to the browsing session.

This indicates remote download/execution activity on WIN10-DH-045 associated with the phishing session. We recommend that you investigate this activity further, as the activity appears to represent an active account takeover and BEC.

References:

1 - https://blog.sekoia.io/tycoon-2fa-an-in-depth-analysis-of-the-latest-version-of-the-aitm-phishing-kit/
2 - https://urlscan.io/result/1876f332-e54f-4d24-9a42-d703e80cc9ec/

Key Details:

User: erik.nilsen@datahaven.no
Host: WIN10-DH-045
Internal IP: 10.4.23.87
External IPs:
- 85.214.12.99 (phishing host A record)
- 89.185.80.19 (attacker infrastructure/credential replay)

- 52.96.0.0 (Microsoft address space observed)
Domain: i9152.cisele0.com
URLs:
- https://i9152.cisele0.com/NOZcbtTxxEiGj/
- https://i9152.cisele0.com/captcha?site=NOZcbtTxxEiGj
- https://i9152.cisele0.com/NOZcbtTxxEiGj/login
WebSocket: wss://i9152.cisele0.com/socket
User-Agents:
- Mozilla/5.0 (Windows NT 10.0; Win64; x64) Chrome/117.0
- Axios/1.7.9
Process Chain: C:\Windows\explorer.exe -> C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
Script Loaded: myscr81234.js (obfuscated)
Event ID: 4624 (Successful interactive logon for user from 89.185.80.19)
OAuth Token Issued: client_id=00000000-0000-0000-0000-000000001337 at 2025-10-28T08:14:40Z
Risk Event: Atypical location (high) for user erik.nilsen@datahaven.no
Credential Replay Traffic: 89.185.80.19 -> login.microsoftonline.com:443
Mailbox Rule: _finance-forward -> ForwardTo attacker-relay@outlook.com
MailItemsAccessed: 7 messages with subject containing "Invoice"
Outbound Email: To finance@victimcorp.no; Subject: Re: Invoice Payment – Urgent; Attachment: payment_request_80295.pdf
Passive DNS: i9152.cisele0.com -> 85.214.12.99 (TTL 300)
WHOIS: i9152.cisele0.com registered 2025-10-18 (privacy-protected)

Consequence:

The incident indicates confirmed account compromise of erik.nilsen@datahaven.no via AiTM, resulting in MFA bypass through session/token replay. The attacker accessed mailbox contents, created a forwarding rule that can exfiltrate sensitive mail, and leveraged the account to conduct Business Email Compromise against external recipients. There is also evidence of suspicious execution on the endpoint during the phishing session, increasing the risk of additional payload delivery. Without prompt containment, the attacker could maintain persistence, expand access via OAuth/Graph, and further abuse trusted communications for financial fraud.

CONTAINMENT

Executed Remediation Actions:

The following containment and eradication actions has been performed by our SOC:
- Isolated host WIN10-DH-045 via EDR to prevent ongoing session hijacking and data exfiltration.
- Terminated suspicious browser-initiated processes and PowerShell on WIN10-DH-045 associated with the phishing session.
- Applied EDR endpoint blocks for domain i9152.cisele0.com and IPs 85.214.12.99 and 89.185.80.19.
- Collected EDR triage artifacts (process tree, network connections, script/module loads) from WIN10-DH-045 for analysis.

- Initiated a full EDR/AV scan on WIN10-DH-045 to detect and remove any additional malicious components.
- Revoked sessions and reset password so that the TA is unable to cause further harm on the account.

Recommended Remediation Actions:

Our SOC recommends that you do the following containment actions:
- Disable the user account erik.nilsen@datahaven.no in AD and Azure AD (Entra ID) immediately.
- Revoke all active sessions/cookies/tokens for the user; invalidate OAuth refresh tokens and remove any malicious OAuth grants.
- Enforce a password reset and require MFA re-enrollment for the user after session revocation.
- Remove the mailbox rule "_finance-forward" and verify no other forwarding rules, delegates, or inbox rules persist.
- Block domain i9152.cisele0.com and IPs 85.214.12.99 and 89.185.80.19 across email gateway, proxy, firewall, and DNS controls.
- Quarantine and recall the outbound BEC message; notify impacted recipients out-of-band to disregard prior payment instructions.
- Review Azure AD sign-in and M365 audit logs for related activity and additional affected accounts; expand session revocation if needed.