Incident Report 2025-11-11

Title:
Date:
Alert Type/Category:
Severity: Low / Medium / High / Critical
Analyst Name:
Case #:

DETECTION AND ANALYSIS

Alert Summary:

We have observed that the user erik.nilsen fell victim to a AiTM phishing attack at 2025-1028. The email sent from support@micr0soft.com (spoofed Microsoft email) was flagged by M365 Defender as a phishing email, but was still delivered to the user's inbox 2025-10-28 08:12:10.

The URL identified by M365 Defender was observed visited by the user at 2025-10-28 08:12:11 in the WebProxy logs, and M365 registered the URL click at 08:12:35. From the proxy logs it can be observed that the user was briefly redirected to the URI /captcha, before being redirected to the URI /NOZcbtTxxEiGj/login. This is consistent with AiTM phishing kits, as they often utilize captchas as part of their anti-forensics techniques to prevent fingerprinting by sandbox engines or similar tools. A WebSocket is then established with wss[:]//i9152.cisele0[.]com/socket and is observed used to proxy the user account details which were submitted as form-data with a POST request at 08:13:50 towards the legitimate Microsoft login oAuth login endpoint (https://login.microsoftonline.com/common/oauth2/authorize). The attackers logs in at 08:17:00 from the American IP 89.185.80[.]19.

Activity from the attacker IP is consistent with Business Email Compromise (BEC). They use Curl to communicate with the Microsof Graph API, and uses it to create and send a phishing email to finance@victimcorp.no. The outbound email has the subject "RE: Invoice Payment - Urgent" and has a document attached named "payment_request_80295.pdf". We also observe the establishment of a forwarding rule named "_finance-forward", that forwards emails to "attacker-relay@outlook.com". This indicates attempts to prevent detection by hiding all (or some) emails from the legitimate user.

Key Details:

User account: erik.nilsen@datahaven.no
Email received from: support@micr0soft.com
Email Subject: Action required: Verify your account
Attacker IP: 89.185.80.19
Attacker User-Agent: Axios/1.7.9
Phishing URL: hxxps[:]//i9152.cisele0.com/NOZcbtTxxEiGj
Outbound email subject: RE: Invoice Payment - Urgent
Outbound email attachment: payment_request_80295.pdf
Outbound email recipients: finance@victimcorp.no

Forwarding rule name: _finance-forward
Forwarding rule destination: attacker-proxy@outlook.com

Consequence:

The account details have been compromised by an attacker and the account was observed misused to spread phishing emails to other companies.
This could lead to further compromises in you own or other companies that trust the sender account.

CONTAINMENT

Executed Remediation Actions:

- No actions applicable

Recommended Remediation Actions:

- Revoke the user account's active sessions
- Reset the account password
- Review and remove malicious forwarding rules in the account's email
- Consider blocking identified IOCs in applicable security measures (e.g. Firewalls)
- Contact recipients and inform about the breach