CTI-rapport: device code phishing waargenomen binnen de zorgsector

TLP: AMBER

Introductie

Het afgelopen jaar waarschuwden diverse organisaties, waaronder Microsoft, voor een toename van device code phishing gericht op Microsoft 365-omgevingen [1][2]. Z-CERT heeft device code phishing inmiddels waargenomen binnen de Nederlandse zorgsector, met name in de context van Business Email Compromise (BEC).

Ook organisaties die hun cloudomgeving beveiligen met bijvoorbeeld phishing-resistente MFA, streng Conditional Access-beleid, geoblocking en IP-allowlisting zijn niet automatisch beschermd tegen deze aanvalstechniek. Het goede nieuws? Een relatief eenvoudige beleidswijziging kan bescherming bieden tegen deze steeds vaker waargenomen aanvalstechniek.

Hoe werkt device code phishing?

Device code authenticatie is bedoeld voor apparaten waarop regulier inloggen minder praktisch is, zoals vergaderapparatuur, smart-tv's of andere apparaten met beperkte invoermogelijkheden. Een apparaat of applicatie vraagt een unieke device code aan bij Microsoft. De gebruiker voert deze code vervolgens in op een tweede apparaat, zoals een laptop of smartphone, op een legitieme Microsoft-inlogpagina. Na succesvolle authenticatie wordt de eerder door het apparaat of de applicatie gestarte sessie geautoriseerd. Handig, want dan hoeft op het apparaat geen wachtwoord meer te worden ingevoerd. **Onhandig: inloggen lukt ook wanneer de sessie door een aanvaller is gestart.**

Bij device code phishing vraagt een aanvaller zelf een geldige device code aan en verleidt vervolgens een gebruiker deze code in te voeren op een legitieme Microsoft-inlogpagina. Nadat de gebruiker succesvol heeft ingelogd en MFA heeft voltooid, krijgt de aanvaller geldige toegangstokens. De aanvaller kan deze tokens vervolgens gebruiken om toegang te verkrijgen tot Microsoft 365-diensten waarvoor het slachtoffer geautoriseerd is.

Hoewel aanvallers vaak gebruikmaken van phishingmails en phishingpagina's om slachtoffers te verleiden een door de aanvaller gegenereerde device code in te voeren, vindt de daadwerkelijke authenticatie plaats op een legitieme Microsoft-inlogpagina. De aanval is daarom niet gericht op het stelen van wachtwoorden, maar op het misbruiken van een legitieme authenticatiestroom.

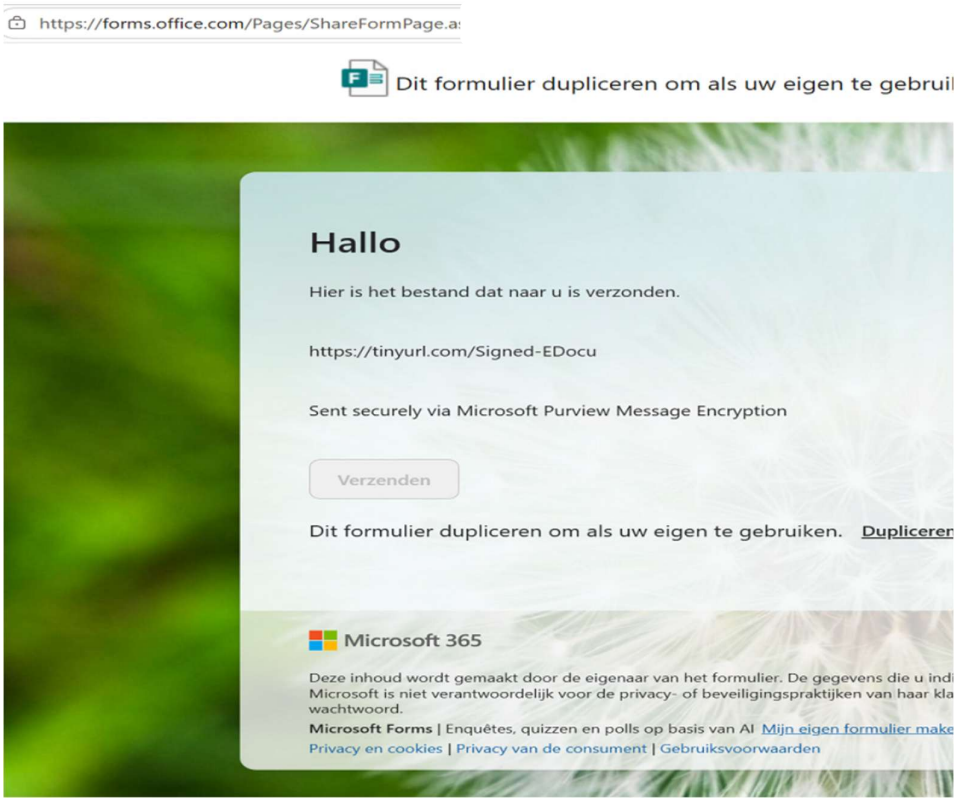
Waargenomen aanvalsketen

Bij Z-CERT zijn meerdere incidenten waargenomen waarbij vermoedelijk gebruik werd gemaakt van de Kali365 Phishing-as-a-Service (PhaaS) kit [4][5]. Deze toolkit werd eerder door Z-CERT waargenomen in campagnes waarbij Adversary-in-the-Middle (AiTM)-technieken werden toegepast. Sinds april 2026 is daarnaast waargenomen dat aanvallers de kit inzetten voor device code phishing.

Stap 1: Misbruik van een vertrouwd e-mailaccount
De aanval start doorgaans met een phishingbericht dat wordt verzonden vanuit een gecompromitteerd e-mailaccount van een vertrouwde zorgorganisatie of leverancier.

Stap 2: Doorverwijzing via een vertrouwde cloudomgeving
Het slachtoffer wordt verleid om via een link een document te bekijken. Die wordt in de e-mail aangeboden via een bijgevoegd pdf-bestand of een pagina binnen een legitieme cloudomgeving waar in de e-mail naar wordt verwezen. Om de uiteindelijke bestemming te verhullen, maken de aanvallers gebruik van een verkorte URL, bijvoorbeeld via TinyURL. Via deze tussenstap wordt het slachtoffer doorgestuurd naar een device code phishingpagina.

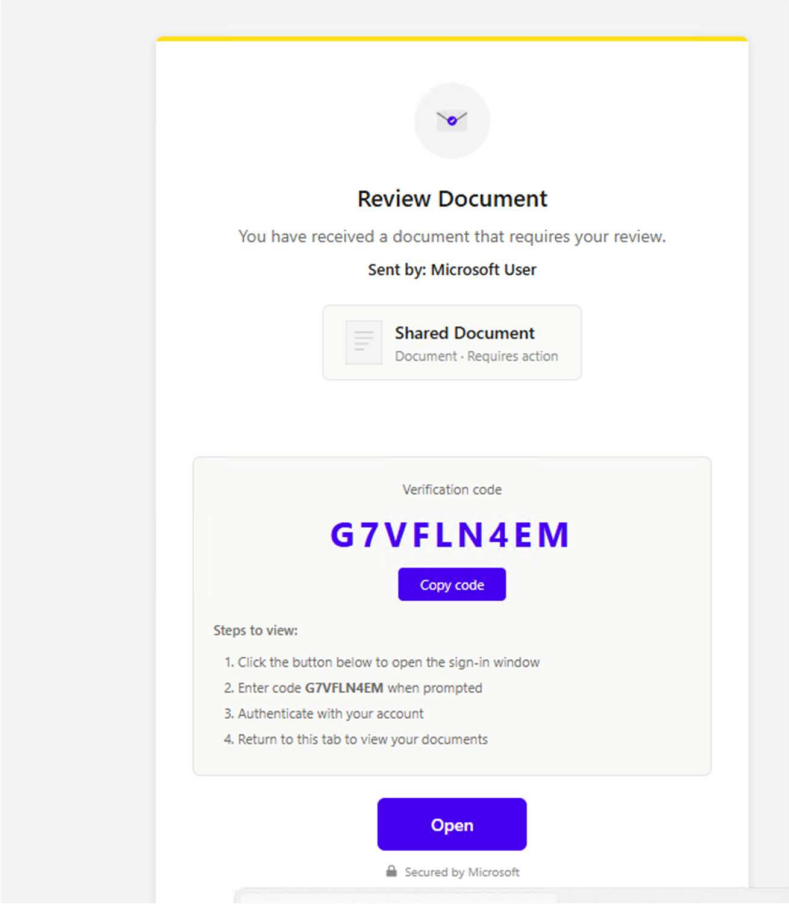
Figuur 1 toont een voorbeeld van deze werkwijze. In dit geval werd een formulier binnen de cloudomgeving van Microsoft gebruikt om een verkorte URL aan te bieden.



Figuur 1. Gebruik van Microsoft Forms als tussenstap naar een device code phishingcampagne.

Stap 3: Device code phishingpagina

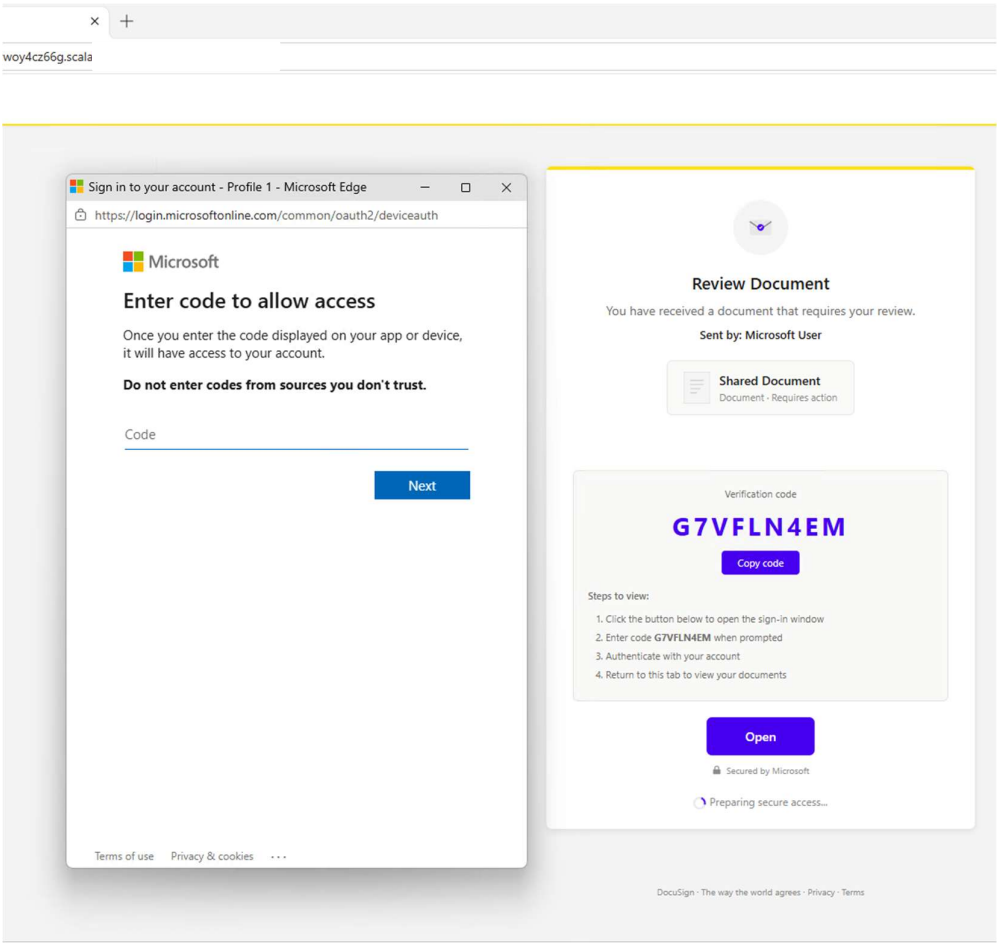
Na het openen van de verkorte URL wordt een device code phishingpagina geladen (figuur 2).
De pagina wekt de indruk dat authenticatie noodzakelijk is om toegang te verkrijgen tot een document. Op de achtergrond heeft de aanvaller echter reeds een device code gegenereerd voor een sessie of apparaat dat onder zijn controle staat.



Figuur 2. Device code phishingpagina die het slachtoffer verleidt een authenticatieproces te starten.

Stap 4: Authenticatie via Microsoft

Wanneer het slachtoffer op **'Open'** klikt, wordt een legitieme Microsoft-authenticatiepagina geopend (figuur 3). Het slachtoffer wordt vervolgens gevraagd de door de aanvaller gegenereerde device code in te voeren en zich te authenticeren. Omdat gebruik wordt gemaakt van een legitieme Microsoft-authenticatiepagina, oogt het authenticatieproces betrouwbaar en ontbreken veel van de gebruikelijke indicatoren van phishing.



Figuur 3. Legitieme Microsoft-authenticatiepagina die wordt gebruikt binnen de device code phishingaanval.

Stap 5: Toegang voor de aanvaller

Feitelijk draait deze authenticatiepoging niet om het verkrijgen van toegang tot een document, maar om het verlenen van toegang aan een apparaat of sessie die onder beheer staat van een kwaadwillende. De aanvaller verkrijgt hierdoor geldige toegangstokens waarmee toegang kan worden verkregen tot Microsoft 365-diensten waarvoor het slachtoffer geautoriseerd is.

Aanbevelingen

Z-CERT adviseert gebruik van de device code authenticatie kritisch te beoordelen. Wanneer deze authenticatiemethode niet noodzakelijk is voor de bedrijfsvoering, kan zij via Conditional Access worden geblokkeerd [3]. Wanneer device code authenticatie wel wordt gebruikt, wordt geadviseerd het gebruik zoveel mogelijk te beperken, passende uitzonderingen te definiëren en actief te monitoren.

Z-CERT adviseert daarbij de volgende werkwijze:

1) Inventariseer
    - Stel vast of device code authenticatie binnen de organisatie legitiem wordt gebruikt door in de Microsoft Entra ID sign-in logs te controleren op aanmeldingen via de Device Code Flow.
    - Bepaal op basis van deze analyse voor welke bedrijfsprocessen of use-cases device code authenticatie daadwerkelijk noodzakelijk is.
2) Beoordeel
    - Beoordeel de impact van het blokkeren van de Device Code Flow, bijvoorbeeld door gebruik te maken van de report-only functionaliteit binnen Conditional Access.
3) Beperk
    - Blokkeer de Device Code Flow via Conditional Access wanneer deze niet noodzakelijk is voor de bedrijfsvoering.
    - Definieer binnen het Conditional Access-beleid eventuele uitzonderingen voor legitiem gebruik van device code authenticatie.
4) Monitor
    - Monitor op afwijkend gebruik van toegestane Device Code Flow-authenticaties.
    - Verwerk relevante device code phishing-indicatoren uit het Zorg Detectie Netwerk (MISP) in detectieregels en monitoring.
5) Bewustwording
    - Neem device code phishing op in awarenessprogramma's en phishingvoorlichting.

Verwachting

Z-CERT verwacht dat device code phishing de komende jaren gemeengoed zal worden omdat de functionaliteit inmiddels opgenomen is in populaire phishingkits [4], waardoor techniek geen barrière meer is. De techniek is aantrekkelijk voor aanvallers omdat zij misbruik maakt van een legitieme authenticatiestroom en daardoor ook succesvol kan zijn tegen goed beveiligde Microsoft 365-omgevingen. Organisaties doen er daarom goed aan het gebruik van device code authenticatie kritisch te beoordelen en waar mogelijk uit te schakelen of te beperken.

Bronnen

[1] Microsoft Digital Defense Report 2025
https://www.microsoft.com/en-us/corporate-responsibility/topics/cybersecurity/reports/microsoft-digital-defense-report-2025/

[2] https://www.proofpoint.com/us/blog/threat-insight/device-code-phishing-evolution-identity-takeover

[3] Microsoft Learn, Block authentication flows with Conditional Access
https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-block-authentication-flows/

[4] https://arcticwolf.com/resources/blog/kali365-expands-into-aws-microsoft-okta-xerox-max-messenger/

[5] https://www.huntress.com/blog/tradecraft-tuesday-device-code-phishing-explained