# Actieve Device code phishing-campagne

| Crisis Notification | TLP:GREEN | Alert Id: 3380c0cf | 2026-09-23 14:52:12 |
|---|---|---|---|

Beste lezer,

Via deze weg willen wij je informeren over een actieve phishing-campagne. Deze campagne heeft op het moment van schrijven al meerdere (zorg-)organisaties getroffen en lijkt zich verder te verspreiden in de gezondheidssector.
Nadat een organisatie slachtoffer is geworden van deze campagne, wordt de phishing-mail verder doorgestuurd naar alle contacten in het adresboek van het slachtoffer. Op deze manier lijkt de phishing-mail van een vertrouwd adres te komen, wat initiële weerbaarheid kan verlagen. Eindgebruikers kunnen mogelijk sneller overtuigd worden om op links te klikken of de acties uit te voeren waarnaar wordt gevraagd.

**Wat gebeurt er?**
De phishing-campagne maakt gebruik van een techniek genaamd “Device Code Phishing”. In de phishing-mail staat een link die de eindgebruiker naar een ‘Microsoft Forms’-formulier stuurt. Vanaf deze pagina wordt de gebruiker gevraagd om nog enkele keren te klikken om een beveiligd document te openen.
De laatste stap in deze keten is het invullen van een “verificatiecode” op de officiële Microsoft-pagina.
Mocht de eindgebruiker deze code invullen, geeft deze effectief toegang tot het Microsoft-account. Omdat de gebruiker alle acties uitvoert binnen de legitieme Microsoft omgeving, worden eventuele mitigaties zoals MFA en Conditional Access Policies omzeild.

**Advies aan gebruikers**
Vul nooit een cijfer- of lettercode in op een Microsoft-pagina wanneer je hier onverwacht per e-mail of ander bericht om wordt gevraagd.
Let hierbij ook op de afzender: een phishingmail kan afkomstig lijken van een bekende of betrouwbare afzender.
Twijfel je over een bericht? Voer de code niet in en neem contact op met je beheerder of servicedesk.
Het laagdrempelig en actief melden kan sterk bijdragen aan het stoppen van verdere verspreiding.
Daarnaast helpt het ons een beter beeld te krijgen van het incident.
Door phishing ben je slachtoffer van misleiding, niet onbekwaam.

**Advies aan beheerders**
Waar mogelijk adviseren we om device code flow uit te schakelen of te beperken binnen de Microsoft-omgeving.
Mocht er sprake zijn, of twijfel bestaan over het slachtoffer zijn van deze campagne, neem dan contact op met Z-CERT. Wij kunnen helpen ondersteunen met het initiële risico beperken en advies over verder onderzoek.

Tenslotte delen wij graag nogmaals ons CTI-rapport over Device Code phishing: https://z-cert.cyware.com/webapp/user/doc-library/ab649c11-2146-4cad-9054-cf1875b4e43e

Hartelijke groet,
Team Z-CERT

**Tags:** Device Code Phishing

**TLP:GREEN:** Informatieverstrekkers kunnen TLP:GREEN gebruiken als het nuttig is om de informatie onder de aandacht te brengen van alle deelnemende organisaties en van alle peers binnen de bredere gemeenschap of sector. Ontvangers mogen TLP:GREEN-informatie met hun peers en met samenwerkende organisaties delen, echter niet via openbaar toegankelijke kanalen. Informatie in deze categorie kan binnen een bepaalde gemeenschap breed worden verspreid. TLP:GREEN-informatie mag niet buiten de gemeenschap openbaar worden gemaakt.