CERT.tg

RÉPUBLIQUE TOGOLAISE
Travail - Liberté - Patrie

ALERTE CYBERSECURITE

ID : ***202601/AP/04***

Alerte – Campagne active de phishing par compromission de comptes Microsoft 365
Date de publication : 23 Février 2026
Niveau de Sévérité : Critique
Type de menace: Phishing, Attaque de « **Man-In-The-Middle** » Type « **Adversary-in-the-Middle** » **(AiTM)**.

Le CERT.tg alerte sur une campagne active de phishing sophistiquée en cours ciblant les environnements Microsoft 365. L'attaque exploite une technique dite « **Adversary-in-the-Middle » (AiTM)** permettant de prendre le contrôle de comptes professionnels même lorsque **l'authentification multifacteur (MFA) est activée**.

[Attention, ***Ne pas cliquer sur les liens*** *contenus dans des notifications de* ***partage SharePoint/OneDrive inattendues****. Vérifier systématiquement auprès de l'expéditeur par un autre* ***canal (téléphone, en personne)****].*

➢ Description de la menace

La victime reçoit un email la **redirigeant vers une fausse page de connexion Microsoft 365**. Cette page est en réalité un proxy contrôlé par l'attaquant qui intercepte **le cookie de session émis** par Microsoft après que la victime a complété son authentification MFA. L'attaquant réutilise ce cookie pour accéder au compte sans mot de passe ni MFA.
Il crée ensuite un **fichier OneNote piégé** contenant un lien de phishing dans le **OneDrive** de la victime, puis **le partage massivement** via **SharePoint** aux contacts professionnels de celle-ci. Les destinataires reçoivent une notification de partage légitime provenant de no-**reply@sharepointonline.com**, rendant la détection très difficile. **Une règle Outlook est créée** pour effacer automatiquement les traces d'envoi. Chaque victime qui clique devient un nouveau vecteur de propagation.

➢ INDICATEURS À SURVEILLER :

- **Notifications de partage SharePoint/OneDrive** inattendues contenant des fichiers **OneNote**
- Fichiers OneNote récents inhabituels dans les OneDrive de vos utilisateurs Partages SharePoint massifs vers un grand nombre de destinataires
- Règles Outlook de **suppression automatique** des « Éléments envoyés » créées sans intervention de l'utilisateur
- Connexions inhabituelles (**IP, géolocalisation**) dans les **Sign-in logs Azure AD / Entra ID**

➢ **MESURES DE PROTECTION RECOMMANDÉES :**

Le CERT.tg invite instamment les organisations à :

1. **Ne pas cliquer** sur les liens contenus dans des notifications de partage SharePoint/OneDrive inattendues. Vérifier systématiquement auprès de l'expéditeur par un autre canal (téléphone, en personne).
2. **Ne jamais saisir** ses identifiants Microsoft 365 après avoir cliqué sur un lien reçu par email. Toujours accéder aux services Microsoft en tapant l'adresse directement dans le navigateur.
3. **Déployer l'accès conditionnel** (Conditional Access) dans Microsoft Entra ID : restreindre les connexions aux appareils conformes et aux localisations autorisées.
4. **Migrer vers un MFA résistant au phishing** : clés de sécurité FIDO2, Windows Hello Entreprise ou certificats (les seules méthodes résistantes aux attaques AiTM).
5. **Activer Microsoft Defender for Office 365** (Safe Links, Safe Attachments) pour l'analyse dynamique des liens et fichiers partagés.
6. **Surveiller les journaux** de connexion (Sign-in logs) et d'audit (Unified Audit Log) de Microsoft 365.
7. **En cas de compromission** : révoquer immédiatement toutes les sessions actives et jetons de rafraîchissement via Entra ID, réinitialiser le mot de passe, supprimer les fichiers et règles Outlook malveillants, et notifier tous les destinataires des fichiers partagés.

Dispositif d'assistance

Les équipes du CERT.tg sont mobilisées pour accompagner les organisations :

- Tél: +228 70 54 93 25
- Site officiel : https://cert.tg/ | Mail : incidents@cert.tg

Le CERT.tg rappelle que la vigilance de chacun contribue à la cybersécurité de tous.

À propos du CERT.tg

Le **CERT.tg** est le **Centre National de Réponse aux Incidents de Cybersécurité au Togo**. Notre mission est de protéger les citoyens, les organisations et les institutions togolaises contre les menaces cybernétiques en assurant la détection, la prévention et la réponse aux incidents de cybersécurité. Ensemble, faisons du Togo un espace numérique sûr et sécurisé.