CERT.tg

RÉPUBLIQUE TOGOLAISE
Travail - Liberté - Patrie

ALERTE CYBERSECURITE

*ID : **202510/AP/19***

Alerte–Campagne de phishing ciblant les cadres et les responsables financiers via LinkedIn
Date de publication : 31 Octobre 2025
Niveau de Sévérité : Elevé
Type de menace : Phishing/hameçonnage

Le CERT-TG alerte sur une nouvelle campagne de phishing par message privé circulant actuellement sur LinkedIn et ciblant spécifiquement des cadres et des responsables financiers. Les attaquants se font passer pour des représentants du **« Conseil d'administration d'un fonds d'investissement international (Common Wealth Investment Fund) »,** en partenariat avec une entité fictive **"AMCO".**
L'objectif est de piéger les victimes par un faux message **LinkedIn**, leur proposant de rejoindre un conseil exécutif prestigieux, afin de voler leurs identifiants Microsoft 365.

Mode opératoire observé :

1. Un message LinkedIn contient une **invitation professionnelle frauduleuse**.
2. Le lien intégré redirige via un **open-redirect Google** vers une page hébergée sur **firebase.storage.googleapis.com,** présentée comme un espace **"LinkedIn Cloud Share"**.
3. Un bouton "**View with Microsoft**" renvoie vers une **fausse page d'authentification Microsoft**, protégée par un **captcha Cloudflare Turnstile** (pour éviter toute détection).
4. Les identifiants saisis sont **transmis aux attaquants**, avec possibilité d'intercepter les cookies de session pour contourner l'authentification multifacteur (MFA).

Indicateurs de compromission (IoCs) :

- Hébergement frauduleux sur : ***.firebase.storage.googleapis.com**
- Redirections via : **google.com/url?sa=**
- Domaines suspects observés : **.icu, .top, .xyz**
- Thèmes de message: ***Board Membership Invitation*, *Common Wealth Investment Fund*, *AMCO Partnership***

Actions recommandées :

1. Sensibiliser les employés sur les messages LinkedIn non sollicités (offres d'emploi, invitations à des réunions/conseils en ligne, propositions de partenariat).
2. Ne jamais saisir d'identifiants après redirection vers des domaines non officiels (vérifier le domaine complet avant connexion).
3. Toujours vérifier l'adresse (URL) du site avant d'y accéder.
4. Activer l'authentification multifactorielle sur les comptes
5. Signaler toute page/URL suspect au CERT TG.
6. Surveiller les journaux Microsoft 365 pour identifier d'éventuelles connexions anormales.

Message du CERT.tg aux entités togolaises
En cas de doute, contactez le CERT.tg :

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

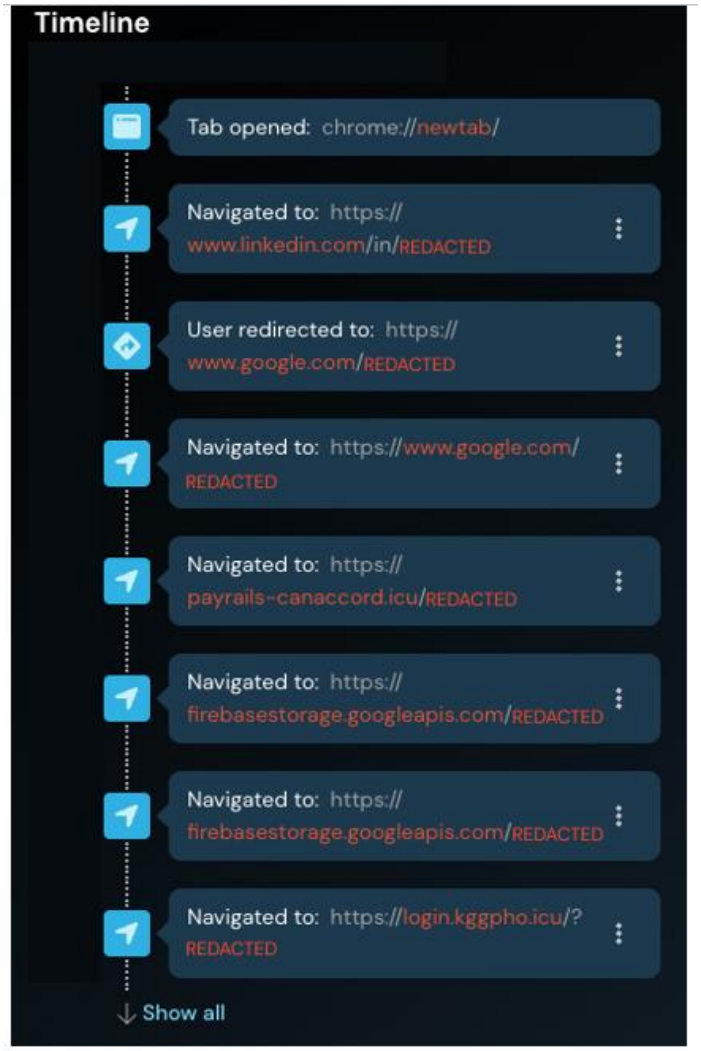
Le CERT.tg rappelle que la vigilance de chacun contribue à la cybersécurité de tous.

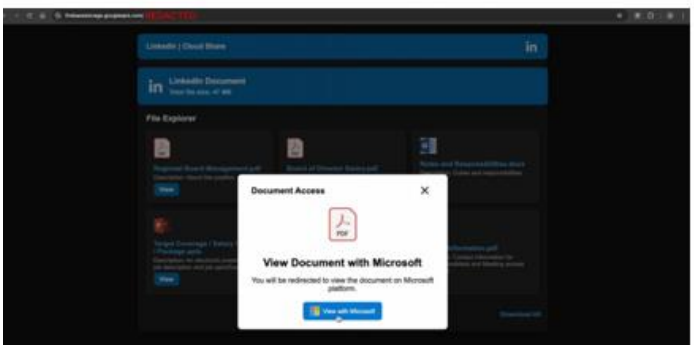
ANCy Agence Nationale de la Cybersécurité

CYBER DEFENSE AFRICA

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.





Chaîne d'attaque observée: redirects-open-redirect Google → Firebase → fausse page Microsoft

Source: https://www.bleepingcomputer.com/

TLP : CLEAR