REPUBLIQUE DU CAMEROUN
Paix - Travail - Patrie
AGENCE NATIONALE DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION
Centre de Reponse Aux Incidents de Securite Informatique

REPUBLIC OF CAMEROON
Peace - Work - Fatherland
NATIONAL AGENCY FOR INFORMATION AND COMMUNICATION TECHNOLOGIES
Computer Incident Response Team

ALERTE DE SECURITE

Campagne de Web Defacement - Groupe ANTONKILL

Date de publication : 08/07/2026

Classification : Publique

Reference : CIRT-AL-2026-07-ANTONKILL

NIVEAU : CRITIQUE

Contexte

Les équipes de sécurité du CIRT ont mis à jour une campagne de cyberattaques de type Web Defacement menée par le groupe cybercriminel nommé ANTONKILL.

Cette campagne a récemment ciblé le site web du Ministère de l'Emploi et de la Formation Professionnelle (MINEFOP), compromettant son image et sa crédibilité. Le groupe exploite des vulnérabilités spécifiques dans le système de gestion de contenu (CMS) Joomla! et le framework Helix3 pour remplacer le contenu légitime par un message de revendication.

Il est impératif que toutes les entités administratives et publiques utilisant ces technologies prennent des mesures immédiates pour sécuriser leurs plateformes.

Analyse de la menace

Le groupe ANTONKILL est un collectif de pirates informatiques actif, probablement basé en Afrique centrale/de l'Ouest, et connu pour une vaste campagne de défiguration de sites web en juillet 2026.

1. mode opératoire

Les utilisateurs malveillants ciblent des sites vulnérables, en se concentrant sur :

- L'exploitation de vulnérabilités dans des plugins ou thèmes obsolètes du CMS Joomla! et du framework Helix3.
- L'injection SQL pour obtenir des accès non autorisés à la base de données du site.
- L'obtention d'accès administrateur via des techniques de force brute ou de phishing.

Une fois le contrôle obtenu, ils injectent un script JavaScript qui affiche une page d'accueil noire avec les caractéristiques suivantes :

Message : "Hacked by Antonkill" (ou variantes comme "trenggalek6etar").

Visuel : Une animation pulsante de crâne (Totenkopf) et des formes géométriques colorées.

Impact : Le contenu original du site est masqué, mais généralement pas supprimé.

2. Cibles Visées

La campagne ne se limite pas au Cameroun. Des cibles internationales ont été identifiées, notamment l'Université Nationale des Sciences et Technologies du Zimbabwe et les Services de Police du Botswana.

INDICATEURS DE COMPROMISSION (IOC)

Bien que des IOC techniques spécifiques tels que adresses IP, hash de fichiers etc ne soient pas encore fourni, les indicateurs comportementaux et contextuels suivants doivent être surveillés :

IOC Comportementaux :

- La détection de pages d'accueil avec un fond noir et un message de revendication ("Hacked by Antonkill").
- L'activité suspecte ou les tentatives d'injection SQL dans les logs du serveur web.
- L'identification de scripts JavaScript inhabituels injectés dans la base de données ou les fichiers de modèle (template) du site.
- Les alertes de force brute sur les interfaces d'administration (ex: /administrator pour Joomla!).

Comment se prémunir ?

Face à cette menace, deux axes d'action prioritaires sont recommandés. Pour les entités potentiellement touchées, des mesures techniques immédiates s'imposent :

- De mettre hors ligne tout site compromis pour stopper la diffusion du message malveillant.
- De lancer une investigation approfondie (scan de vulnérabilités, analyse des logs).
- De vérifier l'intégrité des fichiers (notamment les templates et index.php) et réinitialiser l'ensemble des mots de passe avec une politique renforcée.

Parallèlement, des actions de sécurisation et de prévention concernent toutes les utilisateurs de Joomla! Notamment :

- La mise à jour vers la dernière version stable du CMS, de tous les plugins, extensions et thèmes (en particulier Helix3),
- La suppression des composants inutilisés,
- Le renforcement des accès via l'authentification multi-facteurs et la limitation des tentatives de connexion
- L'activation et la configuration du pare-feu serveur (WAF), mise en place de sauvegardes régulières
- La réalisation d'un audit de sécurité complet.

En complément, des mesures de communication sont essentielles pour gérer la crise entre autres :

- La diffusion d'une alerte en interne auprès des services techniques et de communication et la lecture d'un communiqué officiel destiné au public, afin d'informer de manière transparente sur les faits, les actions entreprises et les conséquences éventuelles.

Ces recommandations, classées par ordre de priorité, visent à endiguer l'attaque, à renforcer durablement la sécurité des plateformes et à maintenir la confiance des utilisateurs.

Conclusion

La campagne ANTONKILL représente une menace sérieuse pour l'intégrité des sites web institutionnels, en particulier ceux fonctionnant sous Joomla! et Helix3. La veille sécuritaire, l'application rigoureuse des correctifs de sécurité et la mise en place de mesures de détection proactive sont essentielles pour prévenir et contrer ce type d'attaque.

Annexe

Capture d'écran du site web du MINEFOP