CERT.tg

RÉPUBLIQUE TOGOLAISE
Travail - Liberté - Patrie

ALERTE CYBERSECURITE

*ID : **202601/AP/02***

Alerte – Campagne de cyberattaque par le malware Astaroth via WhatsApp Web
Date de publication : 28 Janvier 2026
Niveau de Sévérité : Elevé
Type de menace : Astaroth / Guildma – Cheval de Troie bancaire

Le CERT.tg alerte sur une campagne active de cyberattaque **exploitant WhatsApp Web** pour propager un malware bancaire sophistiqué nommé **Astaroth**.
Cette menace vise principalement les **ordinateurs Windows** et permet le **vol d'identifiants bancaires**, de données sensibles et la **propagation automatique** vers les contacts des victimes.

*[Attention, Ne pas ouvrir de **fichiers zip** ou pièces **jointes inattendues** reçues via WhatsApp, même provenant de contacts connus]*

➢ Description de la menace

Des acteurs malveillants exploitent la confiance accordée à WhatsApp pour diffuser **des fichiers ZIP malveillants**, souvent présentés comme des documents légitimes. Une fois le fichier **téléchargé, extrait, puis exécuté sur un poste Windows, le malware Astaroth est installé silencieusement.**
Après infection, le malware :

- Se connecte à WhatsApp Web,
- Récupère la liste de contacts de la victime,
- Envoie automatiquement des messages malveillants similaires,
- Se propage sans l'intervention ni la connaissance de l'utilisateur.

➢ Capacités du malware Astaroth

Astaroth est un cheval de Troie bancaire sophistiqué, capable de :

- Voler les identifiants bancaires et financiers,
- Intercepter les codes/mots de passe à usage unique (OTP),
- Collecter les cookies de navigation,
- Enregistrer les frappes/saisies clavier (keylogging),
- Surveiller les sessions bancaires actives,
- Faciliter des fraudes financières et des accès non autorisés.

➢ Impacts potentiels

Cette campagne peut entraîner :

- La compromission de comptes bancaires,
- Des pertes financières directes,
- L'usurpation d'identité,
- La propagation rapide du malware au sein d'organisations,

- **Recommandations**
  1. Ne pas ouvrir de **fichiers ZIP** ou **pièces jointes inattendues** reçues via WhatsApp, même provenant de contacts connus.
  2. Se méfier des messages incitant à une action urgente ou à un téléchargement immédiat.
  3. Vérifier régulièrement les sessions **WhatsApp Web actives et se déconnecter de toute session non reconnue**.
  4. Maintenir Windows et les applications à jour avec les derniers correctifs de sécurité.
  5. Utiliser une solution de sécurité fiable et à jour (antivirus / EDR).
  6. Sensibiliser les utilisateurs aux techniques de phishing et d'ingénierie sociale.

Message du CERT.tg aux entités togolaises

En cas d'activité suspecte ou incident lié, contactez le CERT.tg, point de contact national 24h/24:

- 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.