Veille Techno : Cyberattaques – Cheval de Troie Android Crocodilus

Le malware Android Crocodilus, découvert en mars 2025 par Threat Fabric, est devenu une menace mondiale. Initialement actif en Turquie, il s'est rapidement propagé à l'Espagne, l'Amérique du Sud, l'Europe et l'Asie, via des publicités malveillantes déguisées en applications légitimes ou mises à jour de navigateurs.

L'une de ses techniques les plus trompeuses consiste à ajouter de **faux contacts** dans le répertoire des victimes, comme "Support bancaire", "Maman" ou "Papa". Ces ajouts rendent les appels frauduleux plus crédibles, incitant les victimes à divulguer des informations sensibles ou à valider des transactions.

Crocodilus exploite aussi les services d'accessibilité Android pour obtenir des autorisations avancées : captures d'écran, enregistrement des frappes, interception d'applications bancaires et de portefeuilles crypto. Il peut même contourner l'authentification à deux facteurs en interceptant les codes OTP de Google Authenticator.

Cette menace souligne l'importance pour les entreprises de renforcer leur cybersécurité mobile : sensibiliser le personnel, limiter les autorisations des apps, adopter des solutions de sécurité spécialisées et surveiller rigoureusement les accès aux données sensibles.

Sources :

https://www.it-connect.fr/pour-tromper-ses-victimes-le-malware-crocodilus-ajoute-de-faux-contacts-sur-android/

https://www.the-sun.com/tech/14394663/urgent-warning-phone-fake-contact-bank-mum-dad/?utm_source=chatgpt.com