



Une campagne d'hameçonnage, visant des services de messagerie instantanée, ciblant des personnalités de haut rang en Europe est actuellement en cours.

Usage sécurisé des messageries instantanées

Contexte

Une campagne d'hameçonnage, via des services de messagerie instantanée (p.ex. Signal et WhatsApp), ciblant des personnalités de haut rang dans les domaines politique, militaire et diplomatique, ainsi que des journalistes d'investigation, est en cours en Europe.

Modes opératoires des attaques et risques associés

Ces attaques ciblent généralement les comptes des utilisateurs et non les applications elles-mêmes. Elles exploitent en effet des fonctionnalités légitimes des applications de messagerie et reposent principalement sur la manipulation des utilisateurs plutôt que sur l'exploitation de vulnérabilités techniques ou l'introduction de code malveillant.

Une fois l'accès obtenu, les attaquants peuvent consulter des communications sensibles, prendre le contrôle du compte et exploiter les contacts et groupes de discussion pour étendre la compromission et collecter des informations précieuses pour de futures opérations de renseignement.

Premier mode opératoire : prise de contrôle du compte de la victime

Les attaquants se font passer pour le support officiel de l'application de messagerie et envoient un message signalant une activité suspecte ou un risque de fuite de données (cf. message d'exemple figure 1 ci-dessous). Ils demandent ensuite à la victime de transmettre le code de vérification reçu par SMS ainsi que le code PIN de l'application. Une fois ces informations obtenues, ils peuvent prendre le contrôle complet du compte, modifier le numéro de téléphone associé et accéder aux contacts ainsi qu'aux conversations, y compris dans les groupes. Les attaquants peuvent également envoyer des messages au nom de la victime, tandis que celle-ci perd l'accès à son compte.

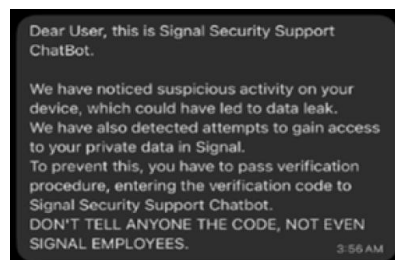


Figure 1

Signal stockant l'historique des conversations localement sur le téléphone, une victime peut retrouver l'accès à cet historique après s'être réenregistrée. La victime peut ainsi penser, à tort, que rien d'anormal ne s'est produit.

Deuxième mode opératoire : appareils liés et codes QR

Dans les applications de messagerie, les codes QR peuvent être utilisés pour ajouter des contacts, partager des informations de contact, rejoindre des groupes de discussion ou associer l'application à d'autres appareils (« appareils liés »).

L'utilisation généralisée de ces codes QR et des liens en fait un moyen attractif pour les attaquants afin d'inciter les victimes à scanner un code ou à cliquer sur un lien. Par exemple, un attaquant peut envoyer un code QR ou un lien à une victime en prétendant l'ajouter à un groupe de discussion, alors que ce code ou ce lien permet en réalité d'associer l'appareil de l'attaquant au compte de la victime.

Cet appareil lié, ou la version de bureau de l'application de messagerie, donne à l'attaquant un accès complet à l'ensemble des conversations de la victime, souvent y compris à l'historique des discussions. L'attaquant peut également lire les messages envoyés par la victime et même envoyer des messages en son nom. La victime conserve l'accès à son compte, mais ne remarque généralement pas immédiatement qu'une autre personne accède à ses communications.

Recommandations

Nous vous invitons à faire preuve d'une vigilance accrue dans l'usage des messageries instantanées et à adopter les neuf réflexes suivants :

1. Ne partagez jamais un code PIN ou un code de vérification avec un tiers, même si la demande semble provenir du support technique de l'application.
2. Restez vigilants face aux messages prétendant provenir d'un service de support ou sollicitant une action urgente ou la transmission d'informations.
3. Ignorez les invitations non sollicitées à rejoindre un groupe de messagerie ou provenant de contacts inconnus.
4. En cas de doute, vérifiez systématiquement l'identité de votre interlocuteur via un autre canal de communication.
5. Ne scannez un QR code que lorsque vous associez volontairement un appareil à votre compte.
6. Vérifiez régulièrement la liste des appareils connectés à vos comptes et déconnectez immédiatement tout appareil que vous ne reconnaissez pas (Signal/WhatsApp : Paramètres → Appareils connectés).
7. Vérifiez régulièrement la composition de vos groupes de messagerie afin d'identifier d'éventuels contacts en double, membres inconnus ou changements inhabituels de nom d'affichage (p.ex. « Deleted account »).
8. Signalez immédiatement tout comportement anormal ou tout compte suspect au helpdesk du CTIE, à votre instance gestionnaire des incidents de sécurité ainsi qu'au délégué à la protection des données de votre entité.
9. Si vous pensez que votre compte a été compromis, informez rapidement vos contacts via un autre canal de communication (p.ex. email ou téléphone).

Pour toute question, nous vous invitons à contacter le HCPN dans sa fonction d'ANSSI par e-mail à l'adresse suivante : support@anssi.etat.lu ou par téléphone au 247-88930.