Le 20 mars 2026

Note d'alerte

Ciblage des messageries instantanées

Le Centre de Coordination des Crises Cyber (C4) observe une recrudescence des campagnes d'attaques visant les comptes de messageries instantanées de personnalités politiques, de hautes autorités et de cadres de l'administration. Les secteurs régaliens sont spécifiquement visés.

L'attaquant peut ainsi avoir **accès à des données sensibles**, telles que l'historique des conversations des personnes ciblées ainsi que le carnet d'adresse de la victime. L'association d'appareils permet aussi à l'attaquant **d'envoyer des messages en usurpant son identité**. Les comptes des victimes peuvent également être utilisés à des fins de désinformation et de manipulation, notamment dans le cadre de manœuvres d'ingérence étrangère.

Ces attaques exploitent un éventuel manque de vigilance amenant une victime à donner des accès à son compte à une tierce personne.

Elles détournent ainsi des fonctionnalités légitimes des messageries, telles que l'association d'appareils (*linked devices*) ou le transfert du compte, afin d'en prendre le contrôle ou simplement d'accéder aux conversations.

Elles sont caractérisées par la réception de messages usurpant l'identité d'un tiers :

- invitant à rejoindre un groupe de discussion en scannant un *QR code*, ce qui aura en réalité pour effet d'associer le compte de messagerie à un appareil contrôlé par l'attaquant ;
- initiant une prise de contact afin, en cas de réponse de la victime, de l'inciter à divulguer des éléments de sécurité (code PIN notamment).

Actions immédiates à effectuer afin de vérifier toute compromission

- **En cas de perte d'accès au compte, le signaler au service chargé de la sécurité informatique.**
- **Vérifier la présence d'appareils associés au compte dans les paramètres de l'application.**
- **En cas de doute, supprimer tous les appareils associés et le signaler au service chargé de la sécurité informatique.** Cette action nécessitera de se reconnecter manuellement sur les appareils tiers appartenant à l'utilisateur légitime du compte.

L'attaquant peut aussi ajouter un compte tiers usurpant l'identité de sa victime dans ses groupes de conversation. Cela permet d'assurer une persistance dans les conversations visées.

- **Vérifier la présence de doublons dans les groupes de discussion des messageries.**
- **En cas de doublon avéré, supprimer du groupe les deux contacts identiques et signaler le compte compromis au service chargé de la sécurité informatique.**

Préconisations générales d'hygiène numérique

Quelle que soit la messagerie utilisée, seule l'adoption de simples mesures d'hygiène informatique permet d'éviter une prise de contrôle des comptes de messagerie par un tiers.

À ce titre, le C4 préconise de :

- **définir un code PIN pour l'application** ;
- **ne jamais répondre à des messages reçus de la part d'individus ou d'entités pour lesquels l'utilisateur de la messagerie n'est pas certain de la véritable identité**. En cas de doute, il convient de vérifier la légitimité du message *via* un autre canal que celui par lequel il a été reçu.

Nota : il convient de préciser que le support technique de ces messageries n'envoie jamais légitimement de messages directs aux utilisateurs.

- **quelle que soit la qualité du correspondant, quand bien même son identité serait confirmée par l'utilisateur :**
  - **ne jamais communiquer des identifiants, des codes PIN ou des mots de passe par ces messageries ;**
  - **ne jamais scanner de QR codes reçus.**
- pour les administrations publiques, **privilégier TCHAP[1] pour les échanges professionnels non sensibles, en lieu et place de messageries instantanées grand public ;**
- **en cas de message suspect ou de doute** (par exemple réception d'une notification suspecte), **contacter le service chargé de la sécurité informatique, qui pourra effectuer un premier niveau de vérification et prendre les mesures nécessaires**.

Les administrations publiques et organisations critiques sont invitées à signaler tout ciblage constaté à l'ANSSI (par téléphone au 3218 ou par courriel : cert-fr@ssi.gouv.fr) ou à la DGSI.

Si la dernière campagne détectée par le C4 – toujours en cours et décrite en annexe – cible la messagerie SIGNAL, **toutes les autres messageries instantanées grand public sont concernées par ce mode opératoire**. À titre d'exemple, WHATSAPP a aussi été ciblée au cours des derniers mois.

[1] Cf. Circulaire demandant l'usage de Tchap (réf. 6497/SG).

Annexe – Exemple d'une campagne d'attaque en cours sur SIGNAL

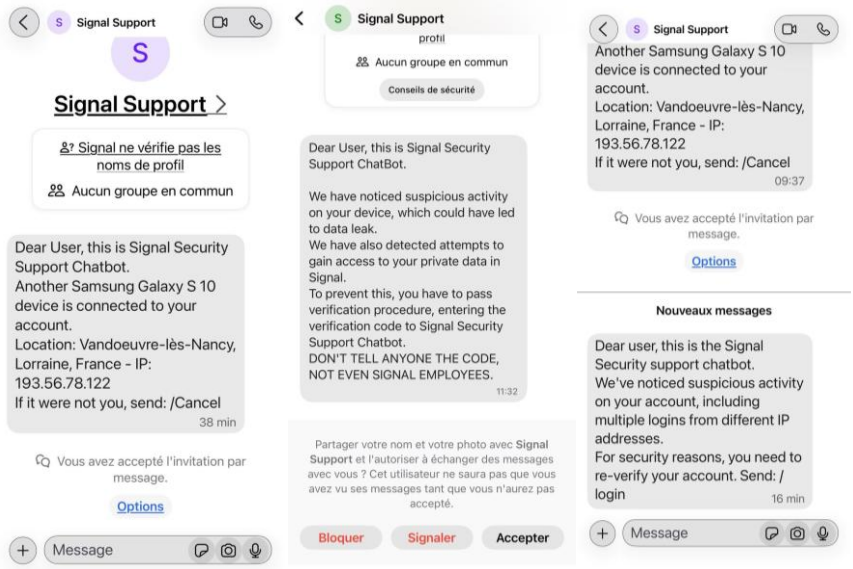
Les investigations du centre de coordination des crises cyber (C4) ont permis de découvrir une campagne d'attaque en cours sur la messagerie instantanée SIGNAL, à l'encontre de personnalités politiques et de cadres de l'Administration, affectant principalement les secteurs régaliens. **Cette note d'alerte du C4 juge particulièrement crédible la publication[2] du 9 mars 2026 par les services néerlandais de renseignement attribuant ces mêmes attaques à des hackers de l'État russe**.

Les attaquants utilisent deux techniques distinctes d'hameçonnage ciblé pour compromettre des comptes SIGNAL. La première, en utilisant les identifiants de la victime et en demandant le code de validation via un faux compte « Support » (approche n°1). Une fois l'opération réalisée, elle permet à l'attaquant de recevoir tous les messages de la victime et d'usurper son identité sur cette messagerie. La seconde *via* la fonctionnalité légitime « appareils liés » ("*linked devices*") de l'application (approche n°2).

Approche n°1

La campagne actuelle est initiée à partir d'un faux compte "Signal Support", prétendant détecter une activité suspecte sur le compte de la cible.

Les captures d'écran ci-après illustrent les différentes tentatives d'approche constatées dans le cas de cette campagne en cours.



Approche n°2

La méthode utilisée par l'attaquant a pour but de lier un compte sur deux appareils. Cette approche existe pour les messageries SIGNAL et WHATSAPP.

Pour cela la victime reçoit un message l'invitant sur un groupe de discussion. En réalité, elle est redirigée vers une fausse page contrôlée par l'attaquant. Afin d'accéder au groupe il est demandé à la victime de procéder à une vérification et de scanner le QR code afin de créer et valider la liaison. Accomplir cette étape valide la liaison de deux comptes à l'insu de la victime (la liaison des comptes est une capacité offerte par SIGNAL permettant d'utiliser un seul compte SIGNAL sur deux terminaux différents). **Cette association de comptes permet ainsi à l'attaquant de recevoir tous les messages ultérieurs de sa cible, et d'envoyer des messages en usurpant son identité**.

[2] **Cybersecurity Advisory. Phishing via messaging apps Signal and WhatsApp -** https://english.aivd.nl/documents/2026/03/09/cybersecurity-advisory.-phishing-via-messaging-apps-signal-and-whatsapp