**ROYAUME DU MAROC**
**ADMINISTRATION**
**DE LA DEFENSE NATIONALE**
**Direction Générale de la Sécurité des Systèmes d'Information**

**المملكة المغربية**
**إدارة الدفاع الوطني**
**المديرية العامة لأمن نظم المعلومات**

## NOTE DE SECURITE

| | |
|---|---|
| **Titre** | Ciblage des messageries instantanées par des groupes malveillants |
| **Numéro de Référence** | 62342403/26 |
| **Date de Publication** | 24 Mars 2026 |
| **Risque** | Critique |
| **Impact** | Critique |

Au cours du mois de mars 2026, plusieurs alertes de sécurité ont signalé des campagnes d'attaque ciblant des applications de messagerie instantanée chiffrées telles que Signal et WhatsApp. Ces opérations sont attribuées à des groupes malveillants organisés et visent principalement des individus présentant un intérêt stratégique, notamment des responsables gouvernementaux, des militaires, des diplomates, des journalistes et des personnels travaillant dans des secteurs sensibles.

L'objectif de ces campagnes est d'accéder aux communications privées des cibles, à leurs listes de contacts et d'utiliser leurs comptes compromis pour mener d'autres attaques. Ces activités s'inscrivent dans des stratégies plus larges de collecte de renseignement, de surveillance et de manipulation de l'information.

Les attaques observées ne cherchent pas à casser le chiffrement de bout en bout des applications de messagerie. Elles reposent plutôt sur l'exploitation des fonctionnalités légitimes des plateformes et sur des techniques d'ingénierie sociale ciblée.

### Usurpation de support et vol de codes de vérification

Les victimes reçoivent des messages se faisant passer pour un service de support ou pour un contact de confiance, leur demandant de partager un code de validation, un mot de passe ou un code PIN. Une fois ces informations obtenues, l'attaquant peut enregistrer le compte de la victime sur un autre appareil et accéder à l'ensemble de ses communications.

### Abus des fonctionnalités de liaison d'appareils

Une autre méthode consiste à envoyer à la victime un lien ou un QR code présenté comme légitime, par exemple pour rejoindre un groupe ou vérifier un compte. En réalité, le scan du QR code ou l'ouverture du lien associe le compte de la victime à un appareil contrôlé par l'attaquant, lui donnant un accès continu aux messages et à la possibilité d'envoyer des communications en son nom.

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

**Impacts potentiels**

La compromission d'un compte de messagerie instantanée peut avoir des conséquences importantes, notamment :

- accès à des échanges sensibles ou confidentiels
- cartographie des relations et des réseaux professionnels de la victime
- diffusion de messages frauduleux depuis un compte légitime
- propagation de l'attaque à d'autres cibles via des messages de confiance
- Dans un contexte étatique, ces compromissions peuvent être utilisées pour soutenir des opérations d'espionnage, de désinformation ou de pression diplomatique.

**Mesures de protection recommandées**

Afin de réduire les risques, plusieurs bonnes pratiques doivent être appliquées :

- ne jamais communiquer de codes de vérification ou d'informations d'authentification via messagerie
- ne pas scanner de QR code reçu de manière inattendue ou provenant d'une source non vérifiée
- examiner régulièrement la liste des appareils connectés à son compte et supprimer ceux qui ne sont pas reconnus
- activer les mécanismes de protection supplémentaires proposés par les applications, comme les codes PIN ou les verrous d'accès

Face à la multiplication des campagnes de compromission ciblant les applications de messagerie instantanée, le maCERT recommande de renforcer les actions de sensibilisation auprès des utilisateurs.

La vigilance des utilisateurs demeure un élément déterminant pour réduire les risques de compromission des comptes et limiter la propagation de ce type d'attaque. Les entités sont invitées à diffuser largement ces messages de prévention auprès de leurs collaborateurs et à rappeler les bonnes pratiques de sécurité liées à l'utilisation des services de messagerie instantanée.

Références :

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

- 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
- CISA, Mobile Communications Best Practice Guidance, d.d. 18 december 2024, https://www.cisa.gov/sites/default/files/2024-12/guidance-mobile-communications-best-practices.pdf
- Phishing Guidance: Stopping the Attack Cycle at Phase One: https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma