AL2026_07 Dutch Government Warns of Signal and WhatsApp Account Hijacking Attacks (March 18th, 2026)

Description

Dutch intelligence agencies have issued a cybersecurity warning regarding a large-scale campaign targeting user accounts on the messaging platforms Signal and WhatsApp.

According to the General Intelligence and Security Service and the Military Intelligence and Security Service, attackers linked to Russian state interests are attempting to hijack accounts used by government officials, diplomats, military personnel, and journalists.

The campaign relies primarily on phishing and social engineering techniques that trick users into revealing authentication codes or linking their messaging accounts to attacker-controlled devices.

Although the encryption mechanisms of the messaging platforms themselves remain secure, compromised user accounts can allow attackers to read conversations, monitor communications, and impersonate victims.

Attack Details

The campaign uses social engineering rather than software vulnerabilities to gain access to messaging accounts.

Key characteristics include:

- **Phishing and impersonation:** Attackers impersonate legitimate support services (such as Signal support chatbots) to convince victims to share verification codes or account PINs.
- **Verification code theft:** Victims are persuaded to disclose one-time authentication codes sent by the messaging platform, allowing attackers to register the account on another device and take control.
- **Abuse of "linked devices" features:** Attackers may trick users into scanning malicious QR codes or linking their accounts to attacker-controlled devices, enabling silent monitoring of conversations.
- **Targeted victims:** The campaign has reportedly targeted government employees, military personnel, diplomats, and journalists, although other individuals of interest may also be affected.
- **Global scope:** Intelligence agencies describe the operation as a large-scale international cyber-espionage campaign aimed at gaining access to sensitive communications.

Because these attacks compromise user accounts rather than the underlying messaging platforms, encrypted communications may still be exposed if attackers successfully gain account access.

Remediation

Organizations and individuals should implement the following measures to reduce the risk of messaging account compromise:

- **Never share verification codes:** Users should never disclose SMS or in-app authentication codes or account PINs to anyone claiming to be support personnel.
- **Verify support communications:** Messaging services such as Signal will not request authentication codes or account credentials through messages, email, or social media.
- **Monitor linked devices:** Regularly review the list of devices linked to messaging accounts and remove any unknown or unauthorized devices.
- **Enable account security features:** Use features such as registration lock, two-step verification, and device authentication when available.
- **User awareness training:** Educate employees about social engineering tactics targeting messaging platforms and remote communication tools.
- **Avoid sharing sensitive information:** Sensitive government, corporate, or classified communications should not be transmitted through consumer messaging applications.
- **Report suspicious activity:** If account compromise is suspected, immediately revoke linked devices, reset credentials, notify contacts, and report the incident to relevant cybersecurity authorities.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- Toulas, B. (2026). *Dutch govt warns of Signal, WhatsApp account hijacking attacks.* Retrieved from BleepingComputer: https://www.bleepingcomputer.com/news/security/dutch-govt-warns-of-signal-whatsapp-account-hijacking-attacks/