ESET Research discovers new spyware posing as messaging apps targeting users in the UAE

DUBAI , DUBAI, UNITED ARAB EMIRATES, October 7, 2025 /EINPresswire.com/ -- ESET researchers have uncovered two Android spyware campaigns targeting individuals interested in secure communication apps, namely Signal and ToTok. These campaigns distribute malware through deceptive websites and social engineering and appear to target residents of the United Arab Emirates (UAE). ESET's investigation led to the discovery of two previously undocumented spyware families: Android/Spy.ProSpy impersonates upgrades or plugins for the Signal app and the controversial and discontinued ToTok app, and Android/Spy.ToSpy impersonates the ToTok app. The ToSpy campaigns are ongoing, as suggested by C&C servers that remain active.

"Neither app containing the spyware was available in official app stores; both required manual installation from third-party websites posing as legitimate services," explains ESET researcher Lukáš Štefanko, who made the discovery. "Notably, one of the websites distributing the ToSpy malware family mimicked the Samsung Galaxy Store, luring users into manually downloading and installing a malicious version of the ToTok app. Once installed, both spyware families maintain persistence and continually exfiltrate sensitive data and files from compromised Android devices. Confirmed detections in the UAE and the use of phishing and fake app stores suggest regionally focused operations with strategic delivery mechanisms."

ESET Research discovered the ProSpy campaign in June 2025, and it has likely been ongoing since 2024. ProSpy is being distributed through three deceptive websites designed to impersonate communication platforms Signal and ToTok. These sites offer malicious APKs posing as improvements, disguised as a Signal Encryption Plugin and ToTok Pro. The use of a domain name ending in the substring ae.net may suggest that the campaign targets individuals residing in the United Arab Emirates, as AE is the two-letter country code for the UAE.

During the investigation, ESET discovered five more malicious APKs using the same spyware codebase, posing as an enhanced version of the ToTok messaging app under the name ToTok Pro. ToTok, a controversial free messaging and calling app developed in the United Arab Emirates, was removed from Google Play and Apple's App Store in December 2019 due to surveillance concerns. Given that its user base is primarily located in the UAE, it is likely that ToTok Pro may be targeting users in this region, who may be more liable to download the app from unofficial sources in their own region.

Upon execution, both malicious apps request permissions to access contacts, SMS messages, and files stored on the device. If these permissions are granted, ProSpy starts exfiltrating data in the background. The Signal Encryption Plugin extracts device information, stored SMS messages, and the contact list, and it exfiltrates other files – such as chat backups, audio, video, and images.

In June 2025, ESET telemetry systems flagged another previously undocumented Android spyware family actively distributed in the wild, originating from a device located in the UAE. ESET labeled the malware Android/Spy.ToSpy. Later investigation revealed four deceptive distribution websites impersonating the ToTok app. Given the app's regional popularity and the impersonation tactics used by the threat actors, it is reasonable to speculate that the primary targets of this spyware campaign are users in the UAE or surrounding regions. In the background, the spyware can collect and exfiltrate the following data: user contacts, device information files such as chat backups, images, documents, audio, and video, among others. ESET findings suggest that the ToSpy campaign likely began in mid-2022.

"Users should remain vigilant when downloading apps from unofficial sources and avoid enabling installation from unknown origins, as well as when installing apps or add-ons outside of official app stores, especially those claiming to enhance trusted services," advises Štefanko.

For a more detailed analysis and technical breakdown of Android/Spy.ProSpy and Android/Spy.ToSpy, check out the latest ESET Research blog post, "New spyware campaigns target privacy-conscious Android users in the UAE" on WeLiveSecurity.com. Make sure to follow ESET Research on Twitter (today known as X), BlueSky, and Mastodon for the latest news from ESET Research.

About ESET
ESET® provides cutting-edge cybersecurity to prevent attacks before they happen. By combining the power of AI and human expertise, ESET stays ahead of emerging global cyberthreats, both known and unknown—securing businesses, critical infrastructure, and individuals. Whether it's endpoint, cloud, or mobile protection, our AI-native, cloud-first solutions and services remain highly effective and easy to use. ESET technology includes robust detection and response, ultra-secure encryption, and multifactor authentication. With 24/7 real-time defense and strong local support, we keep users safe and businesses running without interruption. The ever-evolving digital landscape demands a progressive approach to security: ESET is committed to world-class

research and powerful threat intelligence, backed by R&D centers and a strong global partner network. For more information, visit ESET Middle East or follow us on LinkedIn, Facebook & X.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here