Android Spyware Variant Snoops on WhatsApp, Telegram Messages

By Lindsey O'Donnell

Published: 2020-09-30 · Archived: 2026-04-05 21:57:44 UTC

The Android malware comes from threat group APT-C-23, also known as Two-Tailed Scorpion and Desert Scorpion.

Researchers say they have uncovered a new Android spyware variant with an updated command-and-control communication strategy and extended surveillance capabilities that snoops on social media apps WhatsApp and Telegram.

The malware, Android/SpyC32.A, is currently being used in active campaigns targeting victims in the Middle East. It is a new variant of an existing malware operated by threat group APT-C-23 (also known as Two-Tailed Scorpion and Desert Scorpion). APT-C-23 is known to utilize both Windows and Android components, and has previously targeted victims in the Middle East with apps in order to compromise Android smartphones.

“Our research shows that the APT-C-23 group is still active, enhancing its mobile toolset and running new operations,” according to researchers with ESET in a report released Wednesday. “Android/SpyC32.A – the group’s newest spyware version – features several improvements making it more dangerous to victims.”

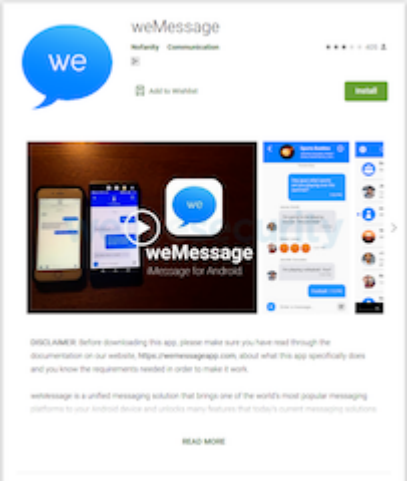
APT-C-23’s activities – including its mobile malware – were first described in 2017 by several security research teams. Meanwhile, the updated version, Android/SpyC23.A, has been in the wild since May 2019 and was first detected by researchers in June 2020.

The detected malware samples were disguised as a legitimate messaging app offered through Google Play. The app, called WeMessage, is malicious, researchers said, and uses entirely different graphics and doesn’t seem to impersonate the legitimate app other than by name. Researchers said, this malicious app does not have any real functionality, and only served as bait for installing the spyware.

Researchers also said they don’t know how this fake WeMessage app was distributed. Previous versions of the malware were distributed in apps via a fake Android app store, called the “DigitalApps” store. The fake app store distributed both legitimate apps as well as fake apps posing as AndroidUpdate, Threema and Telegram. However, researchers said that the fake WeMessage app was not on the “DigitalApps” store.

New Updates

Previously documented versions of this spyware have various capabilities, including the ability to take pictures, record audio, exfiltrate call logs, SMS messages and contacts and more. They would do so by requesting a number of invasive permissions, using social engineering-like techniques to fool technically inexperienced users.



Legitimate WeMessage app. Credit: ESET

This latest version has extended surveillance capabilities, specifically targeting information collected from social media and messaging apps. The spyware can now record victims' screens and take screenshots, record incoming and outgoing calls in WhatsApp and read text of notifications from social media apps, including WhatsApp, Facebook, Skype and Messenger.

The malware also leverages a tactic where it creates a blank screen overlay to put on the Android screen while it makes calls, which helps it hide its call activity. In another technique to hide its activity the malware can dismiss its own notifications. Researchers say this is an unusual feature, possibly used in case of errors or warnings displayed by the malware.

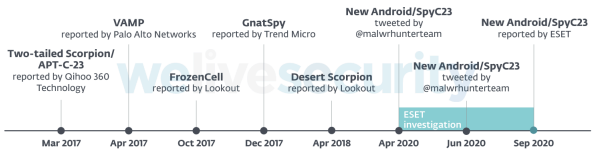
Finally, the new version of the malware can dismiss notifications from built-security security apps for Android devices (allowing it to hide security warnings of suspicious activity from the victim), including Samsung notifications, SecurityLogAgent notifications on Samsung devices, MIUI Security notifications on Xiaomi devices and Phone Manager on Huawei devices.

The malware's C2 communications have also received a facelift. In older versions, the malware used hardcoded C2, either available in plain text or trivially obfuscated – meaning it was easier to identify. In the updated version, however, the C2 is well hidden using various techniques and can be remotely changed by the attacker, making detection much more difficult, researchers said.

Other APT-C-23 Sightings

It's not the first analysis of APT-C-23 this year. At the beginning of 2020, Check Point Research reported new mobile malware attacks attributed to the APT-C-23 group. In April 2020, meanwhile, @malwrhunterteam tweeted about a new Android malware variant, which researchers – in cooperation with @malwrhunterteam – recognized to be part of the APT-C-23 operations. Then in June 2020,

@malwrhunterteam tweeted about another Android malware sample, which was connected to the sample from April.



APT-C-23 malware timeline. Credit: ESET

To avoid falling victim to spyware, researchers advised Android users to only install apps from the official Google Play app store and to scrutinize apps' permissions.

"In cases where privacy concerns, access issues or other restrictions prevent users from following this advice, users should take extra care when downloading apps from unofficial sources," said researchers. "We recommend scrutinizing the app's developer, double-checking the permissions requested, and using a trustworthy and up-to-date mobile security solution."

Source: https://threatpost.com/new-android-spyware-whatsapp-telegram/159694/