APT-C-23 is Still Active and Enhancing its Mobile Spying Capabilities

By Cyware Labs

Published: 2020-10-02 · Archived: 2026-04-06 00:10:15 UTC

APT-C-23, a group of cyber mercenaries known for targeting victims in the Middle East, is still active and enhancing its surveillance capabilities. A recent report from ESET researchers suggests that it has made several deadly improvements to its toolset.

What has been discovered?

The report suggests that it has made several enhancements to its spyware Android/SpyC32.A, and is using it to target victims in the Middle East.

- The new variant of Android/SpyC32.A can snoop on social media apps WhatsApp and Telegram.
- The identified samples were in the guise of genuine messaging app WeMessage, offered through Google Play, but have an entirely different interface from the original app and no real functionality.
- Besides recording Whatsapp calls and reading notifications from social media apps, including Facebook and Skype, the malware can now create screen overlays to put on the Android screen when it makes calls to hide its activities.
- It is also capable of dismissing notifications from built-in security apps, such as SecurityLogAgent notifications (Samsung), MIUI Security notifications (Xiaomi), and Phone Manager (Huawei).

Recent incidents

Desert Falcon has been using the Android/SpyC23.A for its espionage operations since May 2019.

- In June, some samples of Android/SpyC23.A were detected by MalwareHunterTeam, attempting to target client devices in Israel.
- In April, MalwareHunterTeam had detected a new Android malware (later linked to APT-C-23 group), which no security vendor was able to detect besides ESET.

Worth noting

Threat groups such as APT-C-23 seem to have mastered in leveraging sophisticated spyware toolsets to carry out espionage activities. Thus, it becomes important for organizations to stay informed about the latest attack tactics. Experts suggest users to avoid downloading apps from unofficial sources and checking the requested permissions before installing any application.
