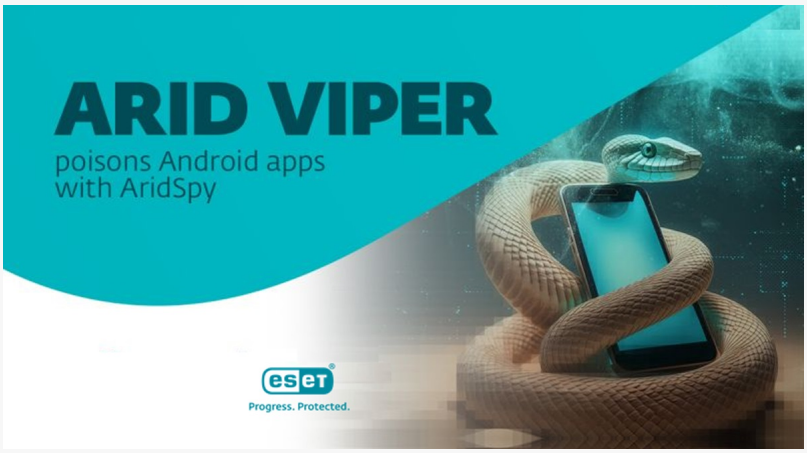
ESET Research: Arid Viper group targets Middle East again, poisons Palestinian app with AridSpy spyware



DUBAI, UNITED ARAB EMIRATES, June 20, 2024 /EINPresswire.com/ -- ESET researchers have identified five campaigns that employ trojanized apps to target Android users. Most likely carried out by the Arid Viper APT group, these campaigns started in 2022, and three of them are still ongoing at the time of publication of this press release. They deploy multistage Android spyware, which ESET has named AridSpy, that downloads first- and second-stage payloads from its Command & Control (C&C) server to assist it in avoiding detection.

The malware is distributed through dedicated websites impersonating various messaging apps, a job opportunity app, and a Palestinian Civil Registry app. Often, these are existing applications that have been trojanized by the addition of AridSpy's malicious code. ESET Research detected the remotely controlled AridSpy Trojan, which focuses on user data espionage, in Palestine and Egypt.

Arid Viper, also known as APT-C-23, Desert Falcons, or Two-tailed Scorpion, is a cyberespionage group known for targeting countries in the Middle East; the group has drawn attention over the years for its vast arsenal of malware for Android, iOS, and Windows platforms.

Three affected apps provided via the impersonating websites are legitimate apps trojanized with AridSpy spyware. These malicious apps have never been offered through Google Play and are downloaded exclusively from third-party sites. To install these apps, the potential victim is asked to enable the non-default Android option to install apps from unknown sources. The majority of the spyware instances registered in Palestine were for the malicious Palestinian Civil Registry app.

"In order to gain initial access to the device, the threat actors try to convince their potential

victim to install a fake, but functional, app. Once the target clicks the site's download button, myScript.js, hosted on the same server, is executed to generate the correct download path for the malicious file," explains ESET researcher Lukáš Štefanko, who discovered AridSpy, describing how users are infected.

One campaign included LapizaChat, a malicious Android messaging application with trojanized versions of StealthChat: Private Messaging bundled with AridSpy's malicious code. ESET identified two other campaigns that started distributing AridSpy after LapizaChat, this time posing as messaging apps named NortirChat and ReblyChat. NortirChat is based on the legitimate Session messaging app, while ReblyChat is based on the legitimate Voxer Walkie Talkie Messenger.

On the other hand, the Palestinian Civil Registry app is inspired by an app previously available on Google Play. However, based on our investigation, the malicious app available online is not a trojanized version of the app on Google Play; instead, it uses that app's legitimate server to retrieve information. This means that Arid Viper was inspired by that app's functionality but created its own client layer that communicates with the legitimate server. Most likely, Arid Viper reverse engineered the legitimate Android app from Google Play and used its server to retrieve victims' data. The final campaign ESET identified distributes AridSpy as a job offering app.

AridSpy has a feature intended to avoid network detection – specifically C&C communication. It can deactivate itself, as AridSpy states in the code. Data exfiltration is initiated either by receiving a command from the Firebase C& C server or when a specifically defined event is triggered. These events include internet connectivity changes, the app is installed or uninstalled, a phone call is made or received, an SMS message is sent or received, a battery charger is connected or disconnected, or the device reboots.

If any of these events occurs, AridSpy starts to gather various victim data and uploads it to the exfiltration C&C server. It can collect the device location; contact lists; call logs; text messages; thumbnails of photos; thumbnails of recorded videos; recorded phone calls; recorded surrounding audio; malware-taken photos; WhatsApp databases that contain exchanged messages and user contacts; bookmarks and search history from the default browser and Chrome, Samsung Browser, and Firefox apps if installed; files from external storage; Facebook Messenger and WhatsApp communication; and all received notifications, among others.

For more technical information about AridSpy, read the blog post "Arid Viper poisons Android apps with AridSpy." Make sure to follow ESET Research on Twitter (today known as X) for the latest news from ESET Research.

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