Indicators of Compromise

accept an inordinate number of permissions.

actor's historical

Android spyware families in SpyC23 forties the connection between this group's various iterations of tools. The

they have applied measures to deter them and remain under the radar. The presence of code from other Arid Viper

Conclusion

We have included additional network indicators associated with app features that are unique to the APKs analyzed,

hostname that uses Western-sounding peoples' names. The primary C2 servers are:

C2 Infrastructure

and further substitution removes spaces and underscores, replacing them with hyphens.

related to manufacturer-specific implementations, including Huawei, Oppo, and Xiaomi.

As the Talos report noted, Skipped was originally a legitimate dating app. The Google Play store version was last

that shares the same Firebase service hostname

There is a non-weaponized version of Skipped Messenger (SHA-1:

prompting.

hurdles for the actor to overcome before a user successfully installs a malicious app. Working the installation flow into a

previously

The theme of these applications center on messaging and communications. We identified two unique themes: one

SpyC23's development; however, there are notable overlaps with these older families and the taxonomy is less distinct.

SentinelLabs compared these newer versions of SpyC23 to the earlier 2020 version, as well as several older Android

mimick Telegram, while another is internally called APP-UPGRADE but is based on a romance-themed messaging app

Through 2022 and early 2023, Arid Viper developed several newer SpyC23 versions that share these themes: two apps

campaign where the actor used a third-party app store to distribute weaponized Android packages (APK). That

one short-lived iOS implant, Phenakite. The SpyC23 Android malware family has existed since at least 2019, though

engaged in

Increased industry focus on Arid Viper is an extension of our continuing collective efforts to track threat actors

posing as Telegram or as a dating app called Skipped.

platform and includes the consistent use and development of mobile spyware since emerging in 2017.

Arid Viper is an espionage-motivated cyber threat actor with Hamas-aligned interests. Arid Viper's toolkit is multi-

package.

package, and the version we discovered on the right houses similar subpackages in the

Java subpackage names: SpyC23 2020 (left) and APP-UPGRADE APK 2023 (right)

platform, the version we discovered on the right houses similar subpackages in the

User In Dangerous Menu" logging messages

©2023 SentinelOne, All Rights Reserved.