ESET Research discovers StrongPity APT group's espionage campaign targeting Android users with trojanized Telegram app

DUBAI, UNITED ARAB EMIRATES, January 17, 2023 /EINPresswire.com/ -- ESET researchers identified an active StrongPity APT group campaign leveraging a fully functional but trojanized version of the legitimate Telegram app, which despite being non-existent, has been repackaged as „the" Shagle app. This StrongPity backdoor has various spying features: its 11 dynamically triggered modules are responsible for recording phone calls, collecting SMS messages, collecting lists of call logs, and contact lists, and much more. These modules are being documented publicly for the very first time. If the victim grants the malicious StrongPity app notification access and accessibility services, the app will also have access to incoming notifications from 17 apps such as Viber, Skype, Gmail, Messenger, and Tinder, and will be able to exfiltrate chat communication from other apps. The campaign is likely very narrowly targeted, since ESET telemetry still hasn't identify any victims.

Unlike the entirely web-based, genuine Shagle site, which doesn't offer an official mobile app to access its services, the copycat site only provides an Android app to download, with no web-based streaming possible. This trojanized Telegram app has never been made available from the Google Play store.

The malicious code, its functionality, class names, and the certificate used to sign the APK file, are the identical to the previous campaign; thus ESET believes with high confidence that this operation belongs to the StrongPity group. Code analysis revealed that the backdoor is modular and additional binary modules are downloaded from the C&C server. This means that the number and type of modules used can be changed at any time to fit the campaign requests when operated by the StrongPity group.

"During our research, the analyzed version of malware available from the copycat website was not active anymore and it was no longer possible to successfully install and trigger its backdoor

functionality. This is because StrongPity hasn't obtained its own API ID for its trojanized Telegram app. But that might change at any time should the threat actor decide to update the malicious app," says Lukáš Štefanko, the ESET researcher who analyzed the trojanized Telegram app.

The repackaged version of Telegram uses the same package name as the legitimate Telegram app. Package names are supposed to be unique IDs for each Android app and must be unique on any given device. This means that if the official Telegram app is already installed on the device of a potential victim, then this backdoored version can't be installed. "This might mean one of two things – either the threat actor first communicates with potential victims and pushes them to uninstall Telegram from their devices if it is installed, or the campaign focuses on countries where Telegram usage is rare for communication," adds Štefanko.

StrongPity's app should have worked just as the official version does for communication, using standard APIs that are well documented on the Telegram website, but it no longer does. Compared to the first StrongPity malware discovered for mobile, this StrongPity backdoor has extended spying features, being able to spy on incoming notifications and exfiltrate chat communication, if the victim grants the app notification access and activates accessibility services.

For more technical information about the latest StrongPity app, check out the blogpost "StrongPity espionage campaign targeting Android users" on WeLiveSecurity. Make sure to follow ESET Research on Twitter for the latest news from ESET Research.

About ESET
For more than 30 years, ESET® has been developing industry-leading IT security software and services to protect businesses, critical infrastructure and consumers worldwide from increasingly sophisticated digital threats. From endpoint and mobile security to endpoint detection and response, as well as encryption and multifactor authentication, ESET's high-performing, easy-to-use solutions unobtrusively protect and monitor 24/7, updating defenses in real time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company that enables the safe use of technology. This is backed by ESET's R&D centers worldwide, working in support of our shared future. For more information, visit www.eset.com or follow us on LinkedIn, Facebook, and Twitter.

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