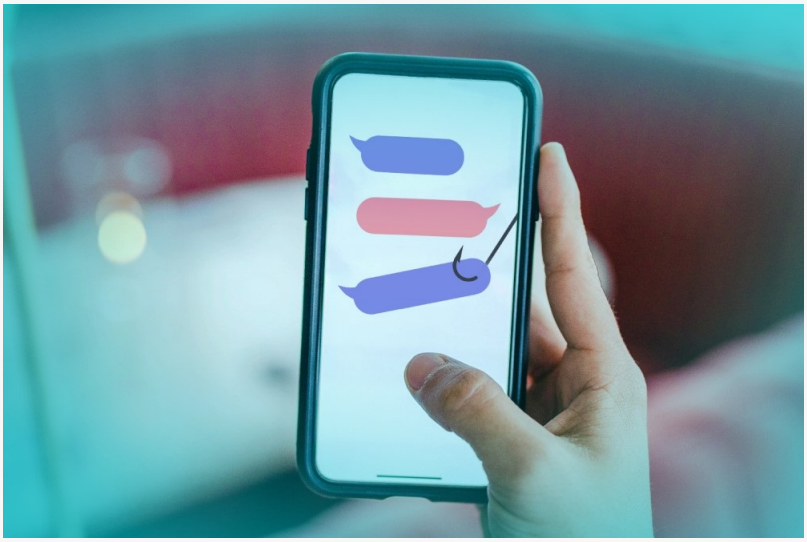
ESET Research: Espionage honey-trap targets officials in India and Pakistan



DUBAI, UNITED ARAB EMIRATES, March 9, 2023 /EINPresswire.com/ -- ESET researchers have analyzed a cyberespionage campaign distributing CapraRAT backdoors through trojanized and supposedly “secure” Android messaging apps that exfiltrate sensitive information. This campaign is still active and is being run by the Transparent Tribe APT group, with the targets being mostly Indian and Pakistani Android users — presumably with a military or political orientation. The victims were probably targeted through a honey-trap romance scam, in which they were initially contacted on another platform and then convinced to use supposedly “more secure” apps, which they were then lured into installing. ESET researchers were able to geolocate over 150 victims from India and Pakistan as well as from Russia, Oman, and Egypt. The threat campaign most likely has been active since July 2022.

“The victims were persuaded to use the MeetsApp or MeetUp app. We have previously seen such honey-trap baits being used by Transparent Tribe operators against their targets. Finding a mobile number or an email address they can use to make first contact is usually not difficult,” explains ESET researcher Lukáš Štefanko, who discovered the campaign. “We identified this campaign when analyzing a different malware sample posted on Twitter,” says Štefanko.

Besides the inherent working chat functionality of the original MeetUp and MeetsApp apps, the trojanized versions include malicious code that ESET has identified as that of the CapraRAT backdoor. Transparent Tribe, also known as APT36, is a cyberespionage group known to use CapraRAT. The backdoor can take screenshots and photos, record phone calls and surrounding audio, and exfiltrate any other sensitive information. The backdoor can also receive commands to download files, make calls, and send SMS messages. The campaign is narrowly targeted, and nothing suggests these apps were ever available on Google Play.

CapraRAT is remotely controlled, executing commands received from the command and control server. Since the operators of these apps had poor operational security, the victims' personally identifiable information was exposed to our researchers across the open internet. It was possible to obtain information about the victims, such as their locations.

Both apps are distributed through two similar websites that describe the apps as secure messaging and calling services. In other words, they pose as the official distribution centers of these apps. Before using the app, victims need to create accounts that are linked to their phone numbers and that require SMS verification. Once this account is created, the app requests further permissions that allow the backdoor's full functionality to work, such as accessing contacts, call logs, SMS messages, external storage, and recording audio.

Transparent Tribe probably uses romance scam baits to lure victims into installing the app and continues to communicate with them using the malicious app to keep them on the platform and make their devices accessible to the attacker.

For more technical information about this latest Transparent Tribe campaign, check out the blog post "Love scam or espionage? Transparent Tribe lures Indian and Pakistani officials" 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