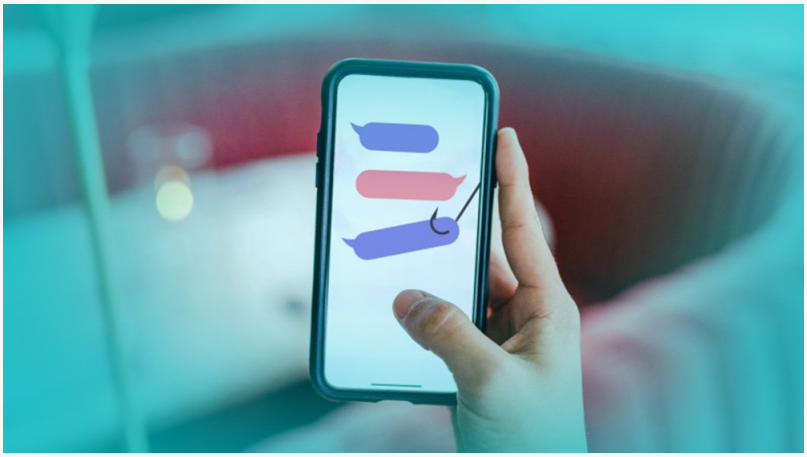
ESET Research discovers espionage apps on the attack in Pakistan, utilizing romance scams



DUBAI , DUBAI, UNITED ARAB EMIRATES, February 5, 2024 /EINPresswire.com/ -- ESET researchers have identified 12 Android espionage apps that share the same malicious code; six were available on Google Play. All the observed applications were advertised as messaging tools, apart from one that posed as a news app. In the background, these apps covertly execute remote access trojan (RAT) code called VajraSpy, used for targeted espionage by the Patchwork APT group. The campaign mostly targeted users in Pakistan. Based on ESET's investigation, the threat actors behind the trojanized apps probably used a honey-trap romance scam to lure their victims into installing the malware.

VajraSpy has a range of espionage functionalities that can be expanded based on the permissions granted to the app bundled with its code. It steals contacts, files, call logs, and SMS messages, but some of its implementations can even extract WhatsApp and Signal messages, record phone calls, and take pictures with the camera.

Based on available numbers, the malicious apps that used to be available on Google Play were downloaded more than 1,400 times. During the ESET investigation, weak operational security of one of the apps led to some victim data being exposed, which allowed researchers to geolocate 148 compromised devices in Pakistan and India. These were likely the actual targets of the attacks. ESET is a member of the App Defense Alliance and an active partner in the malware mitigation program, which aims to quickly find Potentially Harmful Applications and stop them before they ever make it onto Google Play. As a Google App Defense Alliance partner, ESET identified the malicious apps and reported them to Google, and they are no longer available on the Play store. However, the apps are still available on alternative app stores.

Last year, ESET detected a trojanized news app called Rafaqat being used to steal user information. Further research has uncovered several more applications with the same malicious

code. In total, ESET analyzed 12 trojanized apps, six of which (including Rafaqat) had been available on Google Play, and six found in the wild – in the VirusTotal database. These apps had various names, such as Privee Talk, MeetMe, Let's Chat, Quick Chat, Rafaqat, Chit Chat, YohooTalk, TikTalk, Hello Chat, Nidus, GlowChat, and Wave Chat.

To entice their victims, the threat actors likely used targeted honey-trap romance scams, initially contacting the victims on another platform and then convincing them to switch to a trojanized chat application. "Cybercriminals wield social engineering as a powerful weapon. We strongly recommend against clicking any links to download an application that are sent in a chat conversation. It can be hard to stay immune to spurious romantic advances, but it pays off to always be vigilant," advises ESET researcher Lukáš Štefanko, who discovered this Android spyware.

According to the MITRE ATT&CK database, Patchwork has not been definitively attributed and only circumstantial evidence suggests the group may be a pro-Indian or Indian entity. This APT group targets mostly diplomatic and government entities.

For more technical information about VajraSpy and the spying apps from the Patchwork APT group, check out the blog post "VajraSpy: A Patchwork of espionage apps" on WeLiveSecurity.com. Make sure to follow ESET Research on X (formerly known as Twitter) for the latest news from ESET Research.

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

This press release can be viewed online at: https://www.einpresswire.com/article/686240264

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2024 Newsmatics Inc. All Right Reserved.