SpaceCobra group goes after WhatsApp backups using Android spyware GravityRAT, ESET Research discovers

DUBAI, UNITED ARAB EMIRATES, June 16, 2023 /EINPresswire.com/ -- ESET researchers have identified an updated version of the Android-based GravityRAT spyware being distributed as the messaging apps BingeChat and Chatico. GravityRAT is a remote access tool previously used in targeted attacks against users in India. Windows, Android, and macOS versions are available. The actor behind GravityRAT remains unknown; ESET Research tracks the group known as SpaceCobra. Most likely active since August 2022, the BingeChat campaign is still ongoing. In the newly discovered campaign, GravityRAT can exfiltrate WhatsApp backups and receive commands to delete files. The malicious apps also provide legitimate chat functionality based on the open-source OMEMO Instant Messenger app.

Just as in previously documented SpaceCobra campaigns, the Chatico campaign targeted a user in India. The BingeChat app is distributed through a website that requires registration, likely open only when the attackers expect specific victims to visit, possibly with a particular IP address, geolocation, custom URL, or within a specific timeframe. In any case, the campaign is very likely highly targeted.

“We found a website that should provide the malicious app after tapping the DOWNLOAD APP button; however, it requires visitors to log in. We didn’t have credentials, and registrations were closed. It is most probable that the operators only open registration when they expect a specific victim to visit, possibly with a particular IP address, geolocation, custom URL, or within a specific timeframe,” says ESET researcher Lukáš Štefanko, who investigated the malicious apps. “Although we couldn’t download the BingeChat app via the website, we were able to find a distribution URL on VirusTotal,” he adds. The malicious app has never been made available in the Google Play store.

ESET Research does not know how potential victims were lured to, or otherwise discovered, the malicious website. Considering that downloading the app is conditional on having an account and new account registration was not possible during the investigation, ESET believes that potential victims were specifically targeted.

The group behind the malware remains unknown, even though Facebook researchers attribute GravityRAT to a group based in Pakistan, as previously speculated by Cisco Talos. ESET tracks the group under the name SpaceCobra, and attributes both the BingeChat and Chatico campaigns to this group.

As part of the app's legitimate functionality, it provides options to create an account and log in. Before the user signs into the app, GravityRAT starts to interact with its C&C server, exfiltrating the device user's data and waiting for commands to execute. GravityRAT is capable of exfiltrating call logs, contact list, SMS messages, device location, basic device information, and files with specific extensions for pictures, photos, and documents. This version of GravityRAT has two small updates compared to previous, publicly known versions of GravityRAT: exfiltrating WhatsApp backups and receiving commands to delete files.

For more technical information about SpaceCobra and the latest campaign with Android GravityRAT, check out the blogpost "Android GravityRAT goes after WhatsApp backups" 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
0559724623
email us here

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.