ESET Research discovers eXotic Visit campaign, targeted attack via fake messaging apps, available on web and Google Play

DUBAI , DUBAI, UNITED ARAB EMIRATES, April 27, 2024 /EINPresswire.com/ -- ESET researchers have discovered an active espionage campaign targeting Android users with apps primarily posing as messaging services. While these apps offer functional services as bait, they are bundled with the open-source XploitSPY malware. ESET has named this campaign eXotic Visit and has tracked its activities from November 2021 through to the end of 2023. The targeted campaign has been distributing malicious Android apps through dedicated websites and, for a period of time, through the Google Play store as well. Because of the targeted nature of the campaign, the apps available on Google Play had a low number of installs; all of them have been removed from the store. In this likely targeted attack, the eXotic Visit campaign appears to primarily target a select group of Android users in Pakistan and India. There is no indication that this campaign is linked to any known group; however, ESET is tracking the threat actors behind it under the moniker Virtual Invaders.

Apps that contain XploitSPY can extract contact lists and files; extract the device's GPS location; and extract the names of files listed in specific directories related to the camera, downloads, and various messaging apps such as Telegram and WhatsApp. If certain filenames are deemed to be of interest, they can subsequently be extracted from these directories via an additional command from the command and control (C&C) server. Interestingly, the implementation of the chat functionality integrated with XploitSPY is unique; we strongly believe that this chat function was developed by the Virtual Invaders group.

The malware also uses a native library, which is often used in Android app development for improving performance and accessing system features. However, in this case, the library is used to hide sensitive information, like the addresses of the C&C servers, making it harder for security tools to analyze the app. The apps – Dink Messenger, Sim Info, and Defcom – were taken down

from Google Play; moreover, as a Google App Defense Alliance partner, ESET identified ten additional apps that contain code that is based on XploitSPY and shared its findings with Google. Following the ESET alert, the apps were removed from the store. Each of the apps had a low number of installs, suggesting a targeted approach rather than a broad strategy. Overall, around 380 victims have downloaded the apps from websites and Google Play store and created accounts to use their messaging functionality. Because of the targeted nature of the campaign, the number of installs of each app from Google Play is relatively low – between zero and 45.

ESET has identified the malicious code used as a customized version of the open-source Android RAT, XploitSPY. It is bundled with legitimate app functionality, most of the time being a fake, but functioning, messaging application. The campaign has evolved over the years to include obfuscation, emulator detection, and hiding of C&C addresses.

XploitSPY is widely available, and customized versions have been used by multiple threat actors such as the Transparent Tribe APT group, as documented by Meta. However, the modifications found in the apps are distinctive and differ from those in previously documented variants of the XploitSPY malware.

For more technical information about the eXotic Visit campaign, check out the blog post “eXotic Visit campaign: Tracing the footprints of Virtual Invaders”.

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