**Fake Netflix App Discovered Stealing Mobile Files and Reading Text Messages**

A cloud security provider Zscaler has discovered a fake app on third party app stores, posing as the famous television service app, Netflix. After the discovery, Zscaler has advised all smartphone users to download Netflix only from authorized play stores.

The malicious app was found to be a piece of spyware, which the research team named as SpyNote RAT (Remote Access Trojan). This spyware is completely undermining mobile app security by carrying out functions such as; reading SMS messages, viewing contacts, copying device files to a Command and Control Center, executing commands on device, activating microphone and listening to real time conversations.

Once the user installs the fake Netflix app from a third party app store that does not guarantee mobile app security, the spyware-embedded app displays itself with the original Netflix icon on the user’s screen. When the user clicks on the icon for the first time, the icon disappears and seemingly nothing happens. The user thinks that the app may not have been installed correctly and disappeared, but in reality, the spyware has bypassed mobile app security and starts preparing its attacks in the backend.

When contacting the Command and Control server, the spyware makes use of Free DNS services. It also ensures that it continues to spy at the mobile device and does not stop doing so by using the broadcast receivers, services and activities components of Android.

If the hacker decides to run commands on the victim’s device, it can be really troublesome for the latter. By using this feature and a range of vulnerabiliies, the hacker even has the leverage to root the device.

SpyNote RAT can also take screen shots and listen to live audio conversations around the device by turning its microphone on, something that it was already given permission for when the app was being downloaded.

The app was also observed to be stealing SMS, gathering contact details and uninstalling apps. It also only works over WiFi, in order to easily send files to the C & C center.