**Common Free VPN Apps Putting Users at Risk**

Virtual Private Networks intend to keep users safe during online browsing. But a recent study has found that a number of well-known Android VPNs might be exposing users to more risk. This research was a collaborative effort by the Commonwealth Scientific and Industrial Research Organization, University of California and University of New South Wales. The group discovered weak android app security with a large number of vulnerabilities in hundreds of VPNs available on the Google Play Store.

A total of 283 VPN apps were studied. Out of these 38 percent contained malware, 75 percent used a minimum of one thirdparty tracking library, while another 82 percent required permission to access user text messages and accounts.

The researchers scanned for android app security with the help of online scanning service called VirusTotal and determined the app with the most malware. It was found that OkVPN, with only 1000 downloads, was full of malicious content.

At the same time, popular apps such as Butternet with more than five million downloads was also found to be declared malware ridden by 13 different antivirus software programs. One Click VPN with more than a million installs was also flagged by six anti-viruses. About one out of five VPNs do not encrypt their files for protection. 16 percent cannot route user traffic as they don’t have dedicated online servers. Instead, they move through the traffic through other users using the same app.

This is the reason Hola VPN landed in trouble in 2015. It was because of routing user traffic through other users. Hola VPN had about 46 million subscribers at that time, and was surfaced to extreme criticism for not sharing its traffic routing method.

Android app security is suffering at the cost of these insecure VPN accounts. Researchers also figured that 37 percent of analyzed VPNs were installed more than 500, 000 times.