**Bank Details Hacking Android Malware Source Code Leaks Online**

Android users have been warned by security experts to take extraordinary caution when using their financial information on mobile devices after it became known that the source code and instructions of a malware designed to hack banking details of users was leaked online on a forum.

Dr. Web, a Russian anti-malware firm said that “Bank Bot” source code was leaked last month and had already given rise to its variant “dubbed BankBot”, which can quietly hide in a user’s phone and gather all their personal details. Experts at Dr. Web also revealed that the malware can mirror all popular services, such as PayPal. They believe that android app security will be under a serious threat as the number of attacks on Android devices will increase considerably ever since this leak has become known to public.

An extreme threat to android app security, the Trojan exists on third-party app stores, disguising as a Google-related service. Once downloaded, it asks permission to get administrative privilege and if allowed, it gets installed in your system, hides itself from the phone screen by deleting its icon, and connects to the Command and Control server of the criminal for further instructions. It then steals banking credentials from your phone as soon as available.

With its escalated privileges, BankBot enables the attacker to intercept calls, send and intercept text messages, access contact lists, track device location, and much more. It also screens the device for the presence of banking apps like Alfa-Bank, Bank of America, Wells Fargo, etc. at present, the malware mostly seems to target Russian users.

The malware also uses phishing technique to gather banking details of the victim by popping up a screen every time an app like Facebook or Snapchat is launched. The screen resembles official Google’s dialogue box so users who are not usually concerned with android app security fall prey to the hoax and enter their details. The Trojan can also turn off sound and send a text message directly to the cybercriminals without the knowledge of the user.

The researchers have warned that many similar variants of BankBot will now surface after the circulation of the source code. Experts believe that sharing source code and allowing it for modification helps prevent detection.