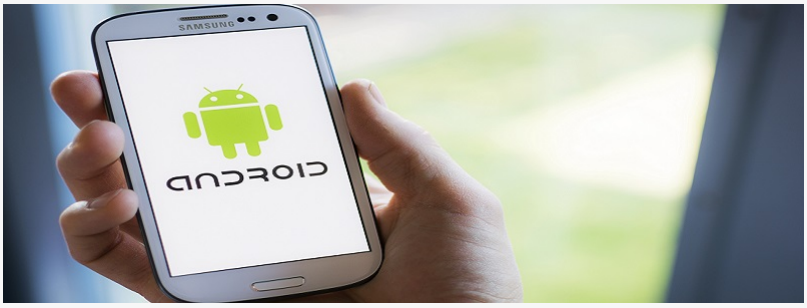
Cyber Criminals Target Android Phones with HeroRAT – REVE Mobile Security Users Safe

HeroRat, an Android remote access Trojan uses Telegram protocol for command, control, and data exfiltration. It is capable of infecting all Android versions.



Android Security

BUKIT BATOK, SINGAPORE, July 6, 2018 /EINPresswire.com/ -- HeroRat is an Android remote access Trojan that uses Telegram protocol for command and control and data exfiltration. Circulated since August 2017, the source code for this malware became publicly available in March 2018 through Telegram hacking channels. This resulted in the creation of hundreds of similar variants being created and distributed.

> We are happy that REVE Mobile Security Antivirus for Android is capable of detecting and quarantining the HeroRat malware. Our users are safe from this malware attack."
>
> *REVE Antivirus CEO Mr. Sanjit Chatterjee*

How does it operate?

Hackers motivate victims to download the malware by flashing attractive offers such as free internet connections, bitcoins, and add on followers on social media. HeroRat has not been able to enter into the Google Play store but it lures victims via social media channels, messaging applications, and 3rd party app stores. Released mostly in Iran, the malware is capable of infecting all Android versions.

However, the users need to accept permissions requested by the app including device administrator privileges to get activated. Once the malware is launched on the device, a message pops up that the application cannot run on it. Hence, it will be uninstalled. This is a fake uninstallation process after which the app icon gets deleted but the victim's device gets registered with the hacker.

Once the attacker gets access to the device of the user, Telegram's bot functionality is used to control the device. The malware is capable of performing multiple functions on the victim's device such as intercepting text messages, screen recording, file exfiltration and fetch device location.

REVE Antivirus malware analysis team has been closely monitoring the malware. REVE Antivirus CEO Mr. Sanjit Chatterjee, commented, "We are happy that REVE Mobile Security Antivirus for Android is capable of detecting and quarantining the HeroRat malware. Our users are safe from this malware attack."

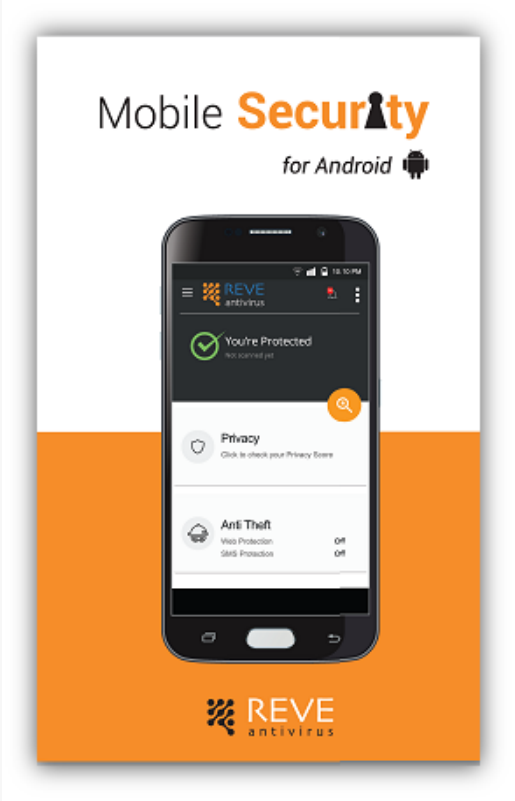
According to REVE Antivirus security experts, malware like HeroRat gets easy access to devices due ignorance of users regarding cybersecurity. PC and mobile users should abstain from downloading

applications and software from 3rd party sites. It's observed that malware enters into the PC/Mobile also as a result of users clicking on links and attachments received on email and messaging apps.

About REVE Antivirus:

REVE Antivirus is a vertical of REVE Group with its headquarters in Singapore & Software Development Centres in India & Bangladesh. A Microsoft approved product, REVE Antivirus has received certification from VB100 a security information portal, testing, and certification body and OPSWAT, a San Francisco-based software company.

Abhijeet Guha
REVE Systems
+919711215965
email us here



Mobile Security for Android

REVE Antivirus