# WhatsApp Pink malware can now auto-reply to your Signal, Telegram texts

WhatsApp malware dubbed WhatsApp Pink has now been updated with advanced capabilities that let this counterfeit Android app automatically respond to your Signal, Telegram, Viber, and Skype messages.

WhatsApp Pink refers to a counterfeit app that appeared this week, primarily targeting WhatsApp users in the Indian subcontinent.

The app touts itself to be a "pink" themed version of the otherwise-green WhatsApp app, but instead contains a trojan that takes over your Android device, and spreads itself to other users.

## WhatsApp Pink spreads via group chat messages

Over the weekend, security researcher Rajshekhar Rajaharia warned WhatsApp users of a new malware circulating via WhatsApp group messages that contain links to scam sites.

These links appear within messages that read like:

Apply New Pink Must Try New WhatsApp. http://XXXXXXXX/?whatsapp

But, clicking on the link takes users to a page where they can download the malicious WhatsApp Pink APK.

As seen by BleepingComputer, the links lead to the following webpage. The "download" button directing the user to the app, WhatsappPink.apk.

WhatsApp Pink is in fact a variant of another malware, a fake Huawei app, that researchers had analyzed earlier this year.

"WhatsApp Pink is an updated version of the WhatsApp auto-reply worm we wrote about in January," said ESET malware researcher, Lukas Stefanko.

"The Trojan's updated version doesn't auto-reply just to WhatsApp messages, but also to messages received on other instant messaging apps, which could be the reason for its apparent wider spread," added the researcher.

**New update auto-replies to your Signal, Telegram, Viber texts**

This week, a video demonstration posted by ESET researchers show that a new update being pushed to the malicious WhatsApp Pink app is capable of auto-responding to your messages from a variety apps including Signal, Viber, Telegram, and Skype.

Although end-to-end encrypted messaging apps like Signal, WhatsApp and Telegram protect communications and messages in transit, like any end-to-end encrypted system, the data at rest can itself be accessible to the person holding the device, or applications (malware) running on the device.

As such, end-to-end encryption should not be misunderstood as protection against compromise of an end device by malicious apps like WhatsApp Pink.

WhatsApp Pink's new update auto-replies to any messages received on Signal, Telegram, WhatsApp, WhatsApp Business, Skype, or Viber with links to the WhatsApp Pink download site so as to spread itself to the unsuspecting users who may click on the link, and download the infected APK.

But, as soon as the app is installed and the user clicks on the WhatsApp Pink app icon, the app disappears, and pretends as if the installation never took place, according to ESET's analysis.

"The victim will then receive a message, to which they will have to reply in order to unwittingly cause it to propagate further."

"Beyond that, however, the new version – detected by ESET products as Android/Spams.V – doesn't really do much," wrote ESET researchers in a blog post.

Stefanko believes that this update could just be a "test" and hint at more malicious variants that are about to come out in the near future.

Users who have downloaded the WhatsApp Pink app can remove it from the Settings and the App Manager submenu, and should ideally scan their Android device with a mobile antivirus solution to ensure the malware removal has succeeded.

**References:**

- https://www.bleepingcomputer.com/news/security/whatsapp-pink-malware-can-now-auto-reply-to-your-signal-telegram-texts/
- https://latesthackingnews.com/2021/04/27/wormable-malware-comes-back-as-whatsapp-pink-now-targets-signal-telegram-too/
- https://www.welivesecurity.com/2021/04/20/whatsapp-pink-watch-out-fake-update/