Check Point discovers new Android virus that spreads via WhatsApp

Check Point Research (CPR) has recently discovered a new malicious threat on the Google Play app store which spreads itself via mobile users' WhatsApp conversations and can also send further malicious content via automated replies to incoming WhatsApp messages.

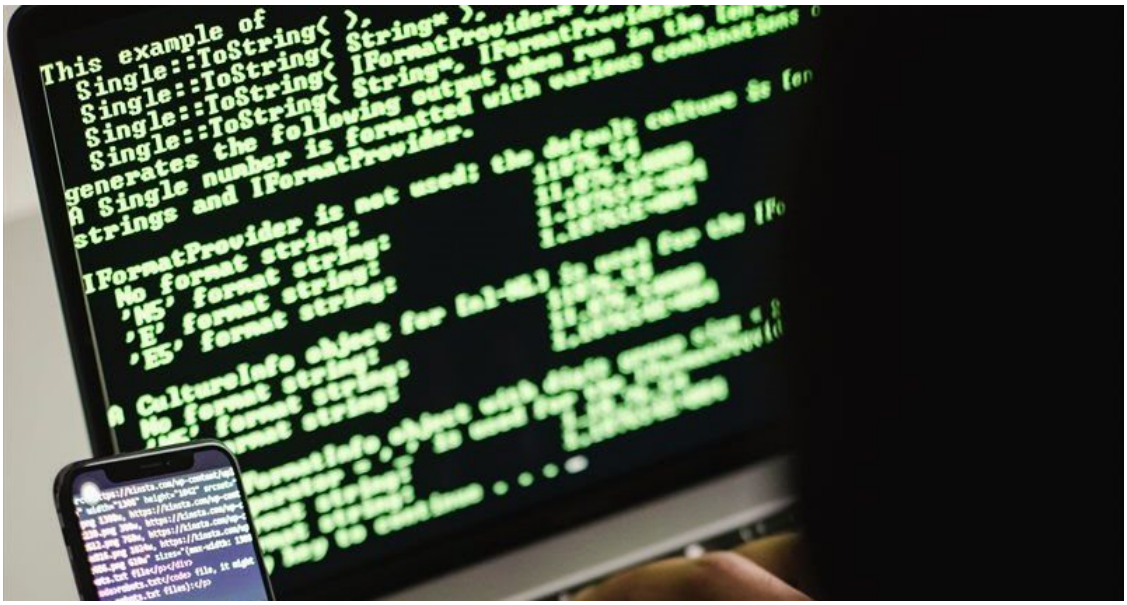

Photo by Sora Shimazaki from Pexels

By replying to incoming WhatsApp messages with a payload from a command-and-control (C&C) server, this method could enable a hacker to distribute phishing attacks, spread further malware, or spread false information or steal credentials and data from users' WhatsApp account and conversations.

Mobile security is a top concern for every company these days - and for a good reason. Over the past year, CPR researchers have observed a rise in the number of mobile-related attacks and new attack methods. From a new malware dropper found on Google Play to an investigation unravelling the Iranian Rampant Kitten APT, the mobile threat landscape is constantly evolving.

A new wormable Android malware, which spreads via WhatsApp auto-replies

As the mobile threat landscape evolves, threat actors are always seeking to develop new techniques to evolve and successfully distribute malware. In this specific campaign, Check Point's researchers discovered a new and innovative malicious threat on the Google Play app store which spreads itself via mobile users' WhatsApp conversations and can also send further malicious content via automated replies to incoming WhatsApp messages.

Researchers found the malware hidden within an app on Google Play called FlixOnline. The app is a fake service that claims to allow users to view Netflix content from all around the world on their mobiles. However, instead of allowing the mobile user to view Netflix content, the application is actually designed to monitor the user's WhatsApp notifications and to send automatic replies to the user's incoming messages using content that it receives from a remote command and control (C&C) server.

The malware sends the following response to its victims, luring them with the offer of a free Netflix service:

> *"2 Months of Netflix Premium Free at no cost for reason of quarantine (Corona virus)* Get 2 Months of Netflix Premium Free anywhere in the world for 60 days."*

Utilising this technique, a threat actor could perform a wide range of malicious activities:

- Spread further malware via malicious links
- Stealing data from users' WhatsApp accounts
- Spreading fake or malicious messages to users' WhatsApp contacts and groups - for example, work-related groups

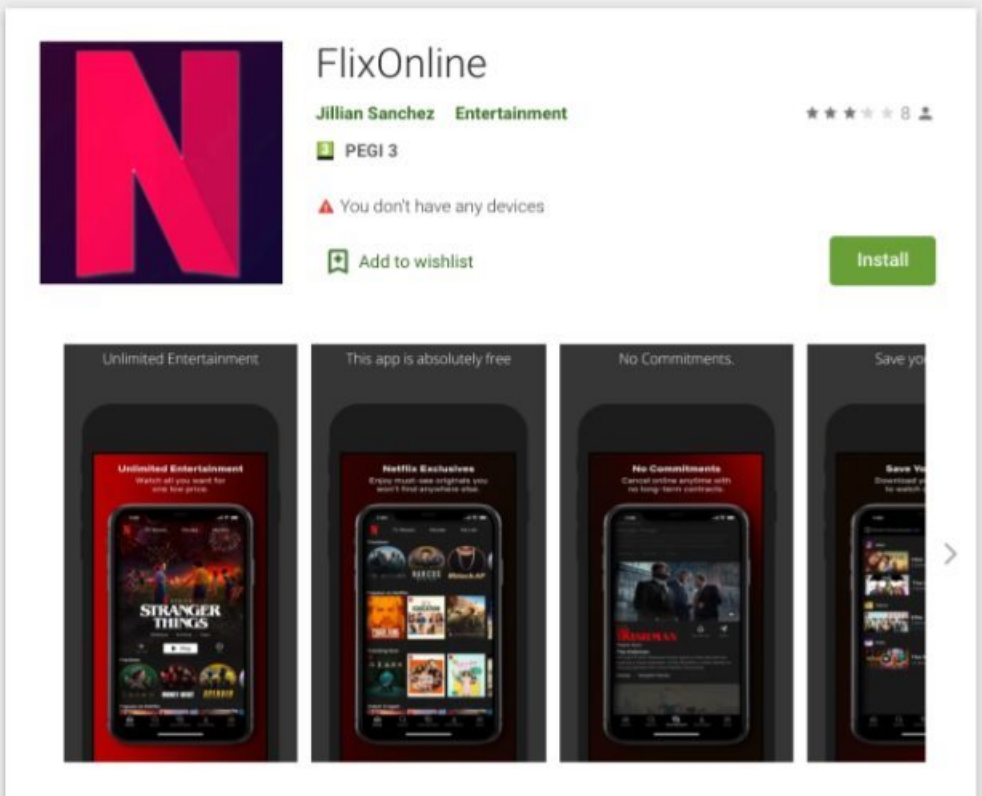

Image supplied

How the malware works

When the application is downloaded from the Play Store and installed, the malware starts a service that requests 'Overlay', 'Battery Optimization Ignore', and 'Notification' permissions. The purpose behind obtaining these permissions is:

- Overlay allows a malicious application to create new windows on top of other applications. This is usually requested by malware to create a fake "Login" screen for other apps, with the aim of stealing the victim's credentials.
- Ignore Battery Optimizations stops the malware from being shut down by the device's battery optimisation routine, even after it is idle for an extended period.

- The most prominent permission is the Notification access, more specifically, the Notification Listener service. Once enabled, this permission provides the malware with access to all notifications related to messages sent to the device, and the ability to automatically perform designated actions such as “dismiss” and “reply” to messages received on the device.

Many faces of malware: Are you protected?

John Mc Loughlin 2 Mar 2021

If these permissions are granted, the malware then has everything it needs to start distributing its malicious payloads and responding to incoming WhatsApp messages with auto-generated replies. Theoretically, through these auto-generated replies, a hacker can steal data, cause business interruptions on work-related chat groups, and even extortion by sending sensitive data to all the user's contacts.

Responsible disclosure

CPR notified Google about the malicious application and the details of its research, and Google quickly removed the application from the Play Store. Over the course of two months, the "FlixOnline" app was downloaded approximately 500 times.

Conclusion

This wormable Android malware features innovative and dangerous new techniques for spreading itself, and for manipulating or stealing data from trusted applications such as WhatsApp. It highlights that users should be wary of download links or attachments that they receive via WhatsApp or other messaging apps, even when they appear to come from trusted contacts or messaging groups.

If a user was infected, they should remove the application from their device, and change their passwords.