New Android malware uses WhatsApp to spread

8 April 2021, by Sarah Katz

Credit: CC0 Public Domain

A new form of Android malware has begun spreading itself by creating auto-replies in WhatsApp. Check Point Research recently discovered the malware in a fake application on Google Play.

Now, any users who have downloaded the malicious application and granted the necessary permissions, the malware can use the auto-reply messages in WhatsApp to send the users an evil payload via a command-and-control (C&C) server. This eclectic strategy could be helping attackers to carry out phishing attacks, steal credentials and WhatsApp data as well as spready false information, among other illicit activities.

The fake app on Google Play was called "FlixOnline," a false service claiming to allow users to utilize the Netflix streaming service from anywhere in the world. However, rather than provide access to Netflix, the app actually interacts with the user's WhatsApp account to send those fake auto-replies. In fact, threat actors can even extort users by threatening to sell their personal WhatsApp conversations and data to all of the users' contacts.

Once a user downloads and installs the application from the Play Store, the malware initiates a service that requests "Overlay," "Battery Optimization Ignore" and "Notification" permissions. Permissions such as Overlay enable attackers to open new windows on top of existing applications for purposes of creating fake login portals to steal user credentials. Batter Optimization Ignore allows the attacker to keep the malware running even after the phone goes idle in order to conserve battery power. Finally, the Notification permission lets attackers view all notifications regarding messages sent to the user's device, including the ability to dismiss or reply to these messages.

Once such permissions are obtained, the malware hides its icon so the software can't be easily deleted. The application conceals itself using updates from the C&C server that routinely changes the malware's configuration. A way this configuration altering might happen involves the C&C server performing an update of the application once the device runs the malware. Specifically, the server uses the OnNotificationPosted callback in order to automatically update the malware.

In fact, as soon as the malware detects a new message notification, the evil app hides the notification from the user so only the malware can view the message. Next, the malware initiates the callback to send the user the fake auto-reply.

Since Check Point Research informed Google about this malicious app, Google has since removed the evil application from the Play Store. Prior to removal, this app was downloaded approximately 500 times.

More information: Hazum, A., et al. "New Wormable Android Malware Spreads by Creating Auto-Replies to Messages in WhatsApp." Check Point Research, Check Point Software

Technologies, 7 Apr. 2021, research.checkpoint.com/2021/n … essages-in-whatsapp/.

© 2021 Science X Network

APA citation: New Android malware uses WhatsApp to spread (2021, April 8) retrieved 29 May 2022 from https://techxplore.com/news/2021-04-android-malware-whatsapp.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.