Joker Trojan

Overview

Joker is a new Trojan on the Google Play store that has been detected in 24 apps with over 472,000 installs in total. It can silently interact with advertising websites that have an offer attached, steal the victim's SMS messages, and pull both contact list and device information. At the time of this document's creation, all 24 apps have been removed from the Google Play Store.

The attacker uses the offers on these ad websites to generate small increments of income by silently accepting the offer on behalf of the victim without his or her knowledge.

How Does it Work?

An infected app will install a Loader by displaying a splash screen, which performs initialization processes silently in the background. Upon completion, the malware will download an obfuscated and AES-encrypted configuration, which is decrypted into a string that contains all necessary information about the core second stage of Joker.

The second stage Core component creates minimal footprint and periodically requests new commands from the C&C server, which are executed in a strict order. Upon receipt of the command message, Joker opens a URL to the ad site with an offer attached, wait for the SMS message with an authorization code to arrive, pulls the code, and enters it into the offer page. Once entered, Joker sends a note to the C&C server that the job is completed, and the process starts again.

Finally, the Core component can collect all numbers in the victim's contact list and send them to the C&C server in encrypted format.

How Lookout Protects and Recommendation for Admins

We recommend blacklisting apps that are infected with Joker. Even though they've been removed from the Play Store, the malware can still work if the app is already installed on a device. As a general best practice, employees should not be installing 3rd party camera and wallpaper apps, which is what most of these are, on work or personal devices.

Lookout Threat Advisory Service

In the fast-changing world of mobile security, keeping your finger on the pulse can be challenging. Lookout Threat Advisory taps into the massive dataset from Lookout's global sensor network of millions of devices, pairing it with insight from its top security researchers to give you actionable intelligence on the latest mobile threats and risks.

Click here to learn more about Lookout Threat Advisory