



# Sharkbot V2



## Overview

In early September 2022, threat researchers discovered multiple Google Play listings for dropper apps which installed the infamous mobile banking trojan *Sharkbot*. Since originally being discovered in late 2021, this Android malware has been used by financially motivated threat actors - targeting both banking apps as well as cryptocurrency apps and exchanges. Recent versions of Sharkbot dropper apps deliver an evolved version of the banking trojan that researchers are referring to as *Sharkbot V2*, and it includes an updated communication mechanism to C2 servers, a domain generation algorithm (DGA) and a fully refactored code base. It also now targets customers of banks in the UK, Italy, Spain, Australia, Poland, Germany, United States of America and Austria.

## Lookout Coverage and Recommendation for Admins

While this particular piece of malware targets mobile banking apps, the same tactic could be used to target accounts for work-related apps like Google Drive, Office 365, and Outlook. This would pose serious risk for any organization that relies on these apps for their employees to be productive from their mobile devices.

Lookout customers are protected against all versions of Sharkbot. Security telemetry from over 170 million mobile apps and 200 million mobile devices helps Lookout automatically detect and protect users against new iterations of existing malware. Admins should be sure that the Trojan policy is enabled in their Lookout console and can choose to alert the device or block it from accessing corporate apps

## Lookout Analysis

The two dropper apps in question, Mister Phone Cleaner and Kylhavy Mobile Security, no longer rely on Accessibility permissions to automatically download and install the Sharkbot trojan. The malware is now installed under the guise of being an update to the two apps. They use a less sophisticated approach than previously-seen Sharkbot droppers, relying on the user unwittingly allowing the installation of the malicious package rather than attempting to implant the payload onto the user's device automatically. This is simpler from a code perspective and likely is a deliberate decision by the threat actors to prevent the dropper's code from being scrutinized. In addition to containing relatively little malicious code, the apps on the Play Store also leverage localization checks to maintain a low profile and limit attempts to drop the malicious package only to devices that match the intended victim profile.

## 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](#)