xHelper

Overview

Xhelper is a new malicious Android dropper app that has infected roughly 45,000 devices in the past six months, with some users reporting that the app reappears on the device, even after the user deletes the app. Additionally, it has the potential to be used to deploy second-stage malware payloads with dangerous capabilities such as stealing user login information, keylogging, deploying ransomware, and bypassing MFA with SMS interception. The majority of victims have been targeted in India, the United States, and Russia.

How Does it Work?

Xhelper can be launched by a variety of external events on the device such as installing an app, connecting to a power supply, or rebooting the device. Once the core functionality is carried out and malicious payload is decrypted to memory, it connects to the C2 server and waits for commands from the attacker. In order to make sure communications between the device and the C2 server remain uninterrupted, SSL certificate pinning is used for all communication, and the server grants the malicious actor a variety of data theft and device takeover options with which to attack the device.

Once the trojan gains access to the target device, Xhelper registers itself as a separate standalone service. It has been reported by some users that the app reappears on the device after it has been uninstalled, though Lookout has not observed this behavior. It's unclear how Xhelper would be able to do this, even if the user spots Xhelper in the Android OS Apps part of the device and removes it manually. The code behind this malware is constantly being updated and shipped out, meaning that it will continue to evolve.

Lookout Coverage and Recommendation for Admins

Lookout Mobile Endpoint Security (MES) and App Defense SDK both provide full coverage of Xhelper and to protect customers against it. The SDK will prevent devices with Xhelper from logging into the integrated customer app, while MES admins can build application-based policies in the platform that will alert both the admin and the end user when they install a trojanized application. This allows them to build in customized remediation tactics to ensure corporate data stays protected. Devices with Lookout installed have been protected against Xhelper apps since September 2019 (some under NecroDrop), and Lookout will continue to research this family and update detection capabilities with its findings.

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