Cerberus Distributed via MDM Breach

Overview

In early May, it was announced that a Mobile Device Management (MDM) platform was breached and malicious actors distributed apps infected with a new variant of the Cerberus trojan to about 75% of a large multinational organization's Android devices. This new variant of Cerberus includes extended remote capabilities that now include logging keystrokes on the device, stealing multifactor authentication (MFA) codes, and controlling the device remotely.

Lookout Analysis

MDM is a combination of apps and configurations, corporate policies and certificates, and backend infrastructure for IT management of mobile devices. While custom-built MDMs have been problematic before, this is the first time that the public has been made aware of a commercially built MDM being breached and leveraged to spread malware. Digging into the root cause of the attack, the two most likely scenarios are that this was an insider threat or that the servers behind the MDM itself were breached. Either way, the Cerberus malware was acquired and custom functionality was built, which is not uncommon for a widely distributed piece of malware like this.

An MDM platform acts as a single point of distribution that can push applications to an entire organization, sometimes without user interaction, which makes it easy for malicious actors to spread malware if the MDM is breached. This is one of many reasons why organizations cannot rely on mobile management products as security products, and that true mobile endpoint security is a necessary part of any company's overall security strategy.

How Lookout Detects and Protects

Lookout will detect and protect against this new variant of Cerberus. Since Cerberus is considered malware-as-a-service, it's easy for malicious actors to acquire it and create new variants of it. However, since the core of the malware remains the same, Lookout customers are protected. There are a number of default policies in Lookout Mobile Endpoint Security that will protect against attacks like Cerberus and other remote access trojans (RATs) like it.

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