Lookout

THREAT GUIDANCE

Simjacker

Overview

AdaptiveMobile Security, a telecom network security provider, uncovered a new and previously undetected vulnerability within SIM cards called Simjacker. According to researchers, this exploit was developed by a private company, but is apparently being leveraged by a government entity to monitor specific individuals. At the time of this document's creation, Simjacker is now being called into question as outside researchers believe it to be limited in reach due to its reliance on legacy technology.

How Does it Work?

The primary exploit involves a specially crafted SMS message sent to the target device which tells the target device to send certain data location and device identifiers such as the IMEI to another attacker controlled mobile phone. The user is completely unaware of the attack and that information was accessed and exfiltrated. The primary data exfiltrated is the target's general location, specifically cellular location data.

This attack is OS-agnostic, meaning it can target both iOS and Android devices. With it, attackers can potentially open a web browser, which researchers believe would likely rely on the S@T browser software as an execution environment, which they've seen being used by mobile operators in over 30 countries.

Lookout Recommendation for Admins

The responsibility for protecting against a SIM-based attack relies on the mobile operators. This is a classic attack against carrier infrastructure, Lookout protections focus on threats from mobile phishing, mobile applications and device risks. This is a highly targeted attack to gather the target's location data, and research shows only an attack on the SIM itself rather than at the device OS level or above. Carrying out this attack requires the attacker to be very knowledgeable about the SIM card stack and carrier infrastructure.

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