LightSpy

Overview

Recently, news broke of a watering hole attack utilizing a fully remote iOS exploit chain to deploy a malware family known as LightSpy on iOS devices up to version 12.2. Dubbed Poisoned News, the campaign was also discovered to use similar capabilities to exploit Android devices using malware named dmsSpy. The goal is to compromise as many mobile devices as possible for surveillance of citizens in Hong Kong. The campaign has been attributed to a new APT group called TwoSail Junk.

Analysis

Like all watering-hole campaigns, this one leverages malicious websites that trick visitors with targeted content. This campaign posts links on multiple online forums that draw interest from Hong Kong residents, and leads them to some sites that were created specifically for this campaign and others that are legitimate but were compromised by the malicious actors. For example, the original watering hole site seen in January was meant to mimic a well-known Hong Kong newspaper called Daily Apple.

Using topics such as Coronavirus or general clickbait, the links would lead the user to legitimate-looking websites that leveraged a Safari bug that allows for exploitation of the well-known vulnerability CVE-2019-8605, which allows iOS devices to be jailbroken, but was patched by Apple in the next software update. In this case, LightSpy allows the attacker to remotely execute shell commands in order to manipulate device files. Other functionalities include the extracting contacts, the Keychain, SMS messages, GPS location, browsing history, and local network IP addresses. It can also leverage modules that exfiltrate data from popular messaging platforms.

How Lookout Detects and Protects

Lookout Phishing and Content Protection will flag and block any of the URLs associated with this campaign. Since Lookout blocks the connection to the malicious URL, the LightSpy payload would not be able to be delivered as part of the Poisoned News. Lookout Mobile Endpoint Security currently detects and protects against the Android version of LightSpy, and iOS coverage will be activated in the next version of our client, expected in early April. Lookout admins should leverage the default “OS Out of Date” protection policy to either warn the end user or block them from accessing corporate infrastructure altogether unless they install the most updated OS, which is not susceptible to these attacks.

Lookout Threat Advisory Service

Threat Advisory combines data from Lookout’s industry-leading dataset and global sensor network of tens of millions of devices to provide its customers with a direct line into the fast-changing world of mobile security. Take advantage of Threat Advisory to gain access to exclusive security intelligence research and immediately actionable insights that your team can use to stay ahead of the malicious actors and keep your organization safe.

Click here to learn more about Lookout Threat Advisory