Mobile APT

Overview

Recently, news broke of Amazon's CEO's phone being hacked via a video sent on WhatsApp. The responsible account is linked to the Saudi Crown Prince and sent the seemingly harmless file, which ended up being malicious. FTI Consulting conducted a forensic investigation of the device after the rate of data leaving the CEO's phone increased exponentially after he clicked the video file. While FTI didn't confirm many specifics of the investigation, this greatly resembles advanced mobile malware similar to Pegasus.

Lookout Analysis

Lookout worked together with Citizen Lab to first discover and analyze Pegasus back in 2016. Since then, Lookout has provided threat-behavior-based detections to protect against similar mobile Advanced Persistent Threats (APTs) similar to Pegasus such as eSurvAgent, Monokle, and ViperRAT.

Lookout Mobile Endpoint Security (MES) and Phishing & Content Protection (PCP) can both protect a device in this scenario in unique ways. MES will detect and protect a compromised device and malware associated with threats like APTs. PCP will monitor the web traffic to and from the device to ensure it's not communicating with and Command and Control (C2) servers or other known malicious websites

Lookout Recommendations for Admins

In order to ensure protection against APTs and similar attacks, Lookout Admins should ensure that all default policies are enabled in the Lookout Console. These policies cover scenarios such as data leakage, connection to malicious content, unknowingly downloading surveillanceware, and other behavior that an APT might engage in without the end user's knowledge or consent. If the Admin's organization has access to Phishing and Content Protection, they should be sure that making PCP mandatory is switched to on in that section of the Protections tab in the Lookout console

Lookout Threat Advisory Service

Threat Advisory combines the 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 malicious actors and keep your organization safe.

Click here to learn more about Lookout Threat Advisory