Operation Triangulation

Overview

Triangulation malware is now known to be in use against Kaspersky employees for at least four years. It was delivered using invisible iMessage texts by attaching a malicious file that exploited OS-level vulnerabilities of iOS without needing any user action. Once these devices were infected, they were a fully-featured APT (advanced persistent threat) platform using a second payload, as described by Kaspersky researchers. The malware has self-destructing properties where the initial text message that started the infection chain gets deleted after the spyware is installed. The installation and data transmission is hidden. It is known to transmit microphone recordings, photos, geolocation, and other data related to the activities of the device owner to remote servers. The malware uses a technique called Canvas Fingerprinting to deduce the hardware-software combination of the device before execution. Kaspersky notes that iOS 15.7 is the latest OS version that was successfully compromised, and there are no indications of the exploits working in more recent iOS versions.

Lookout Coverage and Recommendation for Admins

Lookout already has a coverage in place for this malware. As the malware is known to affect iphones with iOS 15.7 or below, the out of date OS policy can help protect getting infected or using the existing OS vulnerabilities for the spyware's ability to gain entry. We strongly suggest users to keep their devices on auto update for security fixes as and when they become available. Furthermore, any exploited devices are detected by Lookout's device compromise detection. Our phishing and content protection module also protects users against the C2 servers and initial infection vectors.

Lookout Analysis

Once the devices' initial entry is gained, another payload is downloaded with additional malware from the attackers' servers. Kaspersky reported that the campaign started in 2019 and still is ongoing. While the initial text is wiped out, the signs of infection are sprinkled across the device. These include system file modifications to prevent iOS update installation, deprecated library files, and abnormal data usage. Since these attacks have been found in devices up to iOS 15.7, the later versions of iOS might already have fixed the vulnerabilities used in these attacks. Using the Out of Date OS policy and ensuring that devices have auto-update enabled will help protect the devices.

Further, domains are associated with this attack's malicious activity and additional ones for executing commands for collection. These can be blocked by ensuring Lookout's PCP module is in place and actively protecting the devices. As per Kaspersky's notes, the execution toolset lacks a persistence mechanism though.

Lookout Vulnerability and Patch Management

Lookout Vulnerability and Patch Management enables you to know every version of an operating system and mobile app in your organization. We provide visibility into device risk, whether it is company- or employee-owned, as well as managed or unmanaged.

Click here to learn more about Vulnerability & Patch Management