APP-19 · Mobile Threat Catalogue

Archived: 2026-04-06 03:13:21 UTC

Mobile Threat Catalogue

Audio or Video Surveillance

Contribute

Threat Category: Malicious or privacy-invasive application

ID: APP-19

Threat Description: Starting with Android 6.0, access to the microphone or camera is considered a dangerous permission and each recording attempt must be granted permission by the user at runtime. Similarly, the iOS security model only allows apps granted permission by the user to access the camera or microphone while running in the foreground. Therefore, an app operating in these or newer environments cannot abuse public APIs to initiate a recording outside the user's knowledge. This threat can still be realized following successful exploits of OS vulnerabilities that ultimately provide a malicious app with unauthorized access to those resources (e.g. bypass access control on APIs or direct access to the hardware).

Threat Origin

Not Applicable, See Exploit or CVE Examples

Exploit Examples

Malware designed to take over cameras and record audio enters Google Play [1]

An investigation of Chrysaor Malware on Android [2]

CVE Examples

Not Applicable

Possible Countermeasures

Enterprise

Deploy MAM or MDM solutions with policies that prohibit the side-loading of apps, which may bypass security checks on the app.

Deploy MAM or MDM solutions with policies that prohibit the installation of apps from 3rd party (unofficial) app stores.

Deploy MDM solutions that support geo-fencing of BYOD devices with policies that disable device sensors (e.g., camera, microphone) when the device is being operated in sensitive locations.

Deploy MDM solutions for COPE devices that support disabling device sensors (e.g. camera, microphone) that can be used for recording of nearby activity.

Deploy MAM solutions for COPE devices that support selectively enabling device sensors (e.g. camera, microphone) for a whitelist of trusted enterprise applications that require those functionalities.

Use application threat intelligence data about potential abuse of access to device sensors associated with apps installed on COPE or BYOD devices

Mobile Device User

Use Android Verify Apps feature to identify apps that may abuse access to sensor data to record nearby activity.

Mobile App Developer

To reduce risks of using the app, only request access to the minimal set of shared data stores (e.g., contacts, calendar), OS services (e.g. location services), and device sensors (e.g. camera, microphone) necessary for the app to provide functionality.

References

1. D. Goodin, “Malware designed to take over cameras and record audio enters Google Play”, Ars Technica, 7 Mar. 2014; http://arstechnica.com/security/2014/03/malware-designed-to-take-over-cameras-and-record-audio-enters-google-play/ [accessed 8/25/2016] ↩

2. “An investigation of Chrysaor Malware on Android”, blog, 3 Apr. 2017; https://android-developers.googleblog.com/2017/04/an-investigation-of-chrysaor-malware-on.html [accessed 4/5/2017] ↩
