APP-24 · Mobile Threat Catalogue

Archived: 2026-04-29 07:24:07 UTC

Mobile Threat Catalogue

Covertly Track Device Location

Contribute

Threat Category: Malicious or privacy-invasive application

ID: APP-24

Threat Description: Apps that have been granted permission to Location Services or similar OS-provided services can abuse this permission to report device outside of what may be needed to support legitimate app functionality (e.g. navigation). Device location data may facilitate further attacks such as geo-physical or behavioral tracking of the user.

Threat Origin

Dissecting Android Malware: Characterization and Evolution [1]

Exploit Examples

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.

Use application threat intelligence data about potential abuse of location services associated with apps installed on COPE or BYOD devices

Mobile Device User

Use Android Verify Apps feature to identify apps that may abuse location services.

When apps that require location services (e.g., map services) are not in use, use OS-provided settings to globally disable access to location services

When using untrusted apps that require locations services (e.g., map services), use OS-provided settings to revoke access to location services once the app is no longer in use.

Consider the use of devices that support iOS 14 or higher, in which users can decide whether or not applications have access to precision location of their device.

References

1. Y. Zhou and X. Jiang, “Dissecting Android Malware: Characterization and Evolution”, in Proceedings of the 2012 IEEE Symposium on Security and Privacy, 2012, pp 95-109; http://ieeexplore.ieee.org/document/6234407/?arnumber=6234407 [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] ↩
