APP-43 · Mobile Threat Catalogue

Archived: 2026-04-05 14:16:23 UTC

Mobile Threat Catalogue

Malware Uninstalls Itself

Contribute

Threat Category: Malicious or privacy-invasive application

ID: APP-43

Threat Description: By abusing root privileges, a malicious application could avoid detection by automatically deleting itself (with no user interaction) after executing malicious behaviors. This would reduce the opportunity for detection and identification of the malicious activity, which may further prevent or limit the ability for a victim to recover from the attack.

Threat Origin

An investigation of Chrysaor Malware on Android [1]

Exploit Examples

An investigation of Chrysaor Malware on Android [1]

CVE Examples

Possible Countermeasures

Enterprise

To help reduce the opportunity for attack following availability of patches, ensure timely installation of mobile OS security updates.

On Android devices, to prevent an attacker from remotely installing malicious applications from unknown sources, ensure Security > Unknown Sources is turned off; an enterprise can deploy EMM solutions that enforce a policy to never permit the installation of apps from unknown sources.

To decrease the time-to-detection following the installation of a malicious app, deploy on-device agents that automatically detect the installation of any app and initiate either local (on-device) or remote processes for detection and identification of malware and potentially-harmful applications.

Mobile Device User

To help reduce the opportunity for attack following availability of patches, ensure timely installation of mobile OS security updates.

To reduce the potential of installing malicious applications, download public apps directly from an official app store (e.g., Google Play, iTunes Store).

On Android devices, to prevent an attacker from remotely installing malicious applications from unknown sources, ensure Security > Unknown Sources is turned off; an enterprise can deploy EMM solutions that enforce a policy to never permit the installation of apps from unknown sources.

To decrease the time-to-detection following the installation of a malicious app, deploy on-device agents that automatically detect the installation of any app and initiate either local (on-device) or remote processes for detection and identification of malware and potentially-harmful applications.

References
