ECO-21 · Mobile Threat Catalogue

Archived: 2026-04-05 13:24:56 UTC

Mobile Threat Catalogue

Distributing URLs Pointing to Malicious Applications

Contribute

Threat Category: Mobile Application Store

ID: ECO-21

Threat Description: A popular method of distributing links to malicious applications is direct links to the application files. These links can be distributed over several channels, including QR codes, NFC tags, and SMS messages.

Threat Origin

How to Protect Yourself From Malicious QR Codes [1]

Exploit Examples

Find and Call app becomes first trojan to appear on iOS App Store [2]

An investigation of Chrysaor Malware on Android [^AndroidWebBlog-1]

CVE Examples

Possible Countermeasures

Enterprise

To prevent the installation of malicious applications, prohibit sideloading of apps and the use of unauthorized app stores

To decrease the time to detection, use app threat intelligence data to identify malicious applications installed on devices.

Use features such as Apple iOS Managed Apps, Android for Work, or Samsung KNOX Workspace that provide additional separation between personal apps and enterprise apps to mitigate the impact of malicious behaviors.

Educate users about the risks of activating links in emails or SMS messages, and instead encourage users to identify the app where hosted by an official app store.

References

Source: https://pages.nist.gov/mobile-threat-catalogue/ecosystem-threats/ECO-21.html