AUT-13 · Mobile Threat Catalogue

Archived: 2026-04-05 17:49:43 UTC

Mobile Threat Catalogue

Credential Theft via Keylogging

Contribute

Threat Category: Mobile Operating System

ID: AUT-13

Threat Description: A malicious application that is able to intercept screen tap events while other applications are in the foreground can act as a keylogger, thereby collecting authentication credentials (as well as any other sensitive information, such as PII, entered using the displayed keyboard).

Threat Origin

An investigation of Chrysaor Malware on Android [1]

Exploit Examples

An investigation of Chrysaor Malware on Android [1]

CVE Examples

Possible Countermeasures

Mobile Device User

To reduce the potential of downloading a malicious app, such as a keylogger, only install (or permit the installation of) mobile apps downloaded directly from an official app store (e.g. Apple iTunes Store, Google Play).

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

To detect malicious applications, deploy on-device agents that automatically initiate malware detection for all installed applications.

To decrease the value of captured credentials, enable 2-factor authentication for sensitive services (e.g., online banking) where the second factor is not tied to the same device.

Enterprise

To reduce the potential of downloading a malicious app, such as a keylogger, only install (or permit the installation of) mobile apps downloaded directly from an official app store (e.g. Apple iTunes Store, Google Play).

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

To detect malicious applications, deploy on-device agents that automatically initiate malware detection for all installed applications.

Use tools or device APIs (Android SafetyNet, Samsung Knox hardware-backed remote attestation, or other applicable remote attestation technologies) to detect and block enterprise connectivity from devices until they pass such integrity checks.

References
