# APP-35 · Mobile Threat Catalogue

Archived: 2026-04-29 07:23:17 UTC

## Mobile Threat Catalogue

## Retrieving Sensitive Information from Clipboard

Contribute

**Threat Category:** Malicious or privacy-invasive application

**ID:** APP-35

**Threat Description:** Any app that has been granted, or that has implicit OS-level permission to access the clipboard, may collect data left in the clipboard by other activity. A primary example would be using the device clipboard to copy-and-paste a password from an encrypted file to a form field.

**Threat Origin**

Attacks on Android Clipboard [1]

**Exploit Examples**

Update: XcodeGhost Attacker Can Phish Passwords and Open URLs Through Infected Apps [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 MAM solutions that can restrict access to the device clipboard and similar OS-provided services to a whitelist of trusted apps.

Deploy MAM or container solutions that can restrict communication between trusted and untrusted apps using the device clipboard, copy-and-paste, and similar OS-provided services.

Use application threat intelligence services to identify apps reported to abuse access to the device clipboard or similar OS-provided services to obtain sensitive information.

Use app-vetting tools or services to identify applications that appear to abuse access to the device clipboard or similar OS-provided services to obtain sensitive information.

**Mobile Device User**

Use Android Verify Apps feature to identify potentially harmful apps.

**References**

1. X. Zhang and W. Du, “Attacks on Android Clipboard”, Detection of Intrusions and Malware and Vulnerability Assessment: 11th International Conference, 2014;http://www.cis.syr.edu/~wedu/Research/paper/clipboard_attack_dimva2014.pdf [accessed 8/31/16] ↩

2. C. Xiao, “Update: XcodeGhost Attacker Can Phish Passwords and Open URLs Through Infected Apps”, blog, 18 Sep. 2015;http://researchcenter.paloaltonetworks.com/2015/09/update-xcodeghost-attacker-can-phish-passwords-and-open-urls-though-infected-apps/ [accessed 8/31/16] ↩

---