APP-28 · Mobile Threat Catalogue

Archived: 2026-04-02 10:45:29 UTC

Mobile Threat Catalogue

Encrypting and Ransoming Files

Contribute

Threat Category: Malicious or privacy-invasive application

ID: APP-28

Threat Description: A malicious app with permission to modify files or data stored in shared locations, such as external media or contacts could potentially overwrite an original file or data object with an encoded or encrypted one. The attacker could then demand some form of payment in exchange for returning randomed data to a usable state.

Threat Origin

Not Applicable, See Exploit or CVE Examples

Exploit Examples

New Android Trojan xBot Phishes Credit Cards and Bank Accounts, Encrypts Devices for Ransom [1]

CVE Examples

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 apps that maliciously encrypt user data.

Use app-vetting tools or services to identify apps that maliciously encrypt user data.

Mobile Device User

Use Android Verify Apps feature to identify potentially harmful apps.

References
