# ECO-1 · Mobile Threat Catalogue

Archived: 2026-04-05 21:13:42 UTC

## Mobile Threat Catalogue

## Unauthorized Access to Cloud Backups

Contribute

**Threat Category:** Mobile OS & Vendor Infrastructure

**ID:** ECO-1

**Threat Description:** An attacker gains access to a mobile device's cloud backup.

**Threat Origin**

*Not Applicable, See Exploit or CVE Examples*

**Exploit Examples**

Elcomsoft Phone Breaker [1]

**CVE Examples**

*Not Applicable*

**Possible Countermeasures**

**Mobile Device User**

To prevent an attacker from realizing this threat, disable or do not enable cloud backups for the device, which can be accomplished either through mobile OS settings or for enterprises, MDM device policy settings.

To increase the difficulty of an attacker gaining access to a cloud service account, enable increased authentication requirements, such as two-factor authentication or step-up authentication when initally accessing the account from an unknown device.

Some tools used to access cloud-based device backups leverage cryptographic tokens left on computers or devices used to legitimately access the cloud service (e.g., iCloud); if it is believed an attacker has had access to any such system, invalidate any recovered tokens they may have recovered by changing the authentication credentials for the cloud service.

As knowledge of the authentication credentials for a cloud-based backup service may enable an attacker to gain access, protect cloud service authentication credentials from unauthorized disclosure.

### Enterprise

To prevent an attacker from realizing this threat, disable or do not enable cloud backups for the device, which can be accomplished either through mobile OS settings or for enterprises, MDM device policy settings.

### References

1. Elcomsoft Phone Breaker; https://www.elcomsoft.com/eppb.html [accessed 8/29/2016] ↩

---

Source: https://pages.nist.gov/mobile-threat-catalogue/ecosystem-threats/ECO-1.html