

CASE STUDY

Major Mobile App Store: Malicious App Detection at Platform Scale

CONTEXT

Mobile app store distributing over 3M applications globally. The platform sought to protect users from malicious apps impersonating trusted brands. This case study reflects detection and enforcement activity over a 12-month period.

CHALLENGE

Advanced visual analysis was required to detect adversarial impersonation at platform scale.

OUTCOME

- 2,400+ impersonation apps submitted
- 72% action rate (Suspend / Block / Warning)
- Impersonation detected across 500+ brands
- Flagged scam apps representing 50M+ cumulative installs
- Documented a 30% recurrence rate via version-based evasion

SYSTEM CAPABILITIES DEMONSTRATED

- Advanced visual detection of brand-color mimicry and splashscreen manipulation
- Identification of repeat offenders and published/unpublished state evasion
- Reverse-engineering of mobile app code to uncover hidden trading functionality
- Detection of geolocation-triggered malicious behavior