

Hirudo Android Malware Replaces Banking Apps to Bypass Security Controls



A new Android malware replaces legitimate banking apps with modified versions that disable signature checks, accessibility detection and integrity verification to steal credentials and enable remote control.

- Hirudo malware uninstalls genuine banking apps and replaces them with patched copies that disable security checks using hooking frameworks
- Malware is delivered through seemingly legitimate shopping, adult content or short drama apps that act as loaders
- Modified apps bypass signature verification, hide accessibility services, remove screenshot protection and manipulate Play Integrity checks
- Malware steals banking passwords, payment PINs, SMS messages and provides screen streaming

and camera access to operators

- Targets banking apps in Indonesia, China, India, Mexico, Morocco and Thailand with thousands of credential entries found in unsecured backend

Threat Overview

Mobile security researchers have identified a sophisticated Android malware strain named **Hirudo** that employs an unusual technique to evade banking app security controls. Rather than attempting to overlay or intercept legitimate banking applications, the malware completely replaces them with modified versions that disable built-in security mechanisms.

The malware is distributed through seemingly legitimate applications for shopping, adult content or short drama that function as advertised but serve as loaders. Once installed, these apps display fake update notifications that prompt users to grant accessibility permissions. Hirudo then uninstalls the genuine banking app, downloads a patched copy, and uses accessibility privileges to install the replacement without user awareness.

Technical Evasion Methods

The modified banking apps retain nearly all original code but incorporate a hooking engine built on open-source frameworks. When launched, the patched application substitutes the genuine signing certificate when queried, hides enabled accessibility services from detection, removes screenshot protection to enable remote viewing, and manipulates key-attestation certificates while relaying Play Integrity requests through operator-controlled infrastructure.

Researchers note that the hooking engine runs inside the banking app's own process, effectively turning the application's defenses against itself. However, certain limitations exist: the bundled attestation keybox has been publicly leaked and Google has listed two of its certificates as compromised, making server-side revocation checks capable of detecting these forgeries.

Operational Capabilities and Targeting

Once active, Hirudo can steal banking passwords, payment PINs, device-unlock credentials and SMS messages. The malware provides operators with screen streaming capabilities and access to both device cameras. Fake checkout pages collect payment PINs and display fabricated success messages to deceive victims during data theft.

Researchers observed the malware targeting banking applications in Indonesia, China, India, Mexico, Morocco and Thailand. An unsecured backend panel revealed thousands of application-credential entries along with device, lock-screen and financial-profile data, though the total victim count remains unknown. Security researchers characterize this as a deliberate escalation in Android banking malware, shifting focus from device-level integrity checks to the security mechanisms embedded within banking applications themselves.

What to do now

1. Implement server-side validation of app integrity and attestation checks for all mobile banking transactions
2. Bind integrity verification to user sessions and protected actions rather than relying solely on client-side checks
3. Deploy behavioral analytics and transaction-risk controls that operate independently of client-side app security
4. Review and strengthen mobile app security policies to detect and block installation of apps from unofficial sources
5. Educate customers on the risks of sideloading APK files and granting accessibility permissions to non-system apps
6. Monitor for anomalous patterns such as app reinstallation events followed by unusual transaction activity