

Hirudo Android Trojan Replaces Banking Apps with Patched Versions to Evade Security



A new Android banking trojan replaces legitimate banking apps with patched versions that bypass built-in security checks, representing an escalation in mobile financial fraud targeting Indonesian banks.

- Hirudo trojan replaces legitimate banking apps with patched versions that bypass internal security checks
- Eight Indonesian banking apps have been targeted with replacement versions
- The technique marks a new escalation in mobile financial fraud tactics
- Dutch mobile security firm ThreatFabric identified the threat
- Attack works by circumventing security controls from within the app itself

Threat Overview

Cybersecurity researchers have identified a new Android banking trojan named **Hirudo** that employs an advanced technique to compromise mobile banking security. Unlike traditional banking malware that overlays fake login screens or intercepts credentials, Hirudo replaces legitimate banking applications with specially crafted patched versions designed to bypass the security checks built into the apps themselves.

Dutch mobile security company ThreatFabric disclosed the threat after identifying replacement versions targeting eight Indonesian banking applications. This approach represents a significant escalation in mobile financial fraud tactics, as the malicious apps appear and function like genuine banking software while undermining security controls from within.

Technical Implications

The Hirudo technique circumvents traditional mobile security measures by operating inside what users and many security tools would consider a legitimate banking app. By patching the original application code, threat actors can disable certificate pinning, integrity checks, and other protective mechanisms that banks implement to secure their mobile channels. This allows attackers to intercept communications, manipulate transactions, or extract credentials without triggering the security alerts that would normally protect customers.

Regional Considerations

While current targeting focuses on Indonesian institutions, the technique is portable and could be adapted to banking apps in any market. Saudi financial institutions should note that this attack vector bypasses many conventional mobile security controls and requires a comprehensive approach to mobile application security, user education, and fraud monitoring to detect and prevent similar compromises.

What to do now

1. Review mobile application security architecture to ensure integrity checks, certificate pinning, and anti-tampering controls are properly implemented and cannot be easily bypassed
2. Implement runtime application self-protection (RASP) or similar technologies that detect when banking apps are running in modified or compromised environments
3. Enhance fraud monitoring systems to detect anomalous transaction patterns that may indicate use of compromised or patched mobile applications
4. Educate customers about downloading banking apps only from official app stores and verifying app authenticity before installation
5. Establish procedures to monitor for unauthorized or modified versions of institutional mobile applications appearing in app stores or third-party repositories
6. Coordinate with mobile security vendors to ensure endpoint detection capabilities can identify patched or

repackaged versions of legitimate banking apps