Bazuka: New Android Malware Framework Uses Fake Overlays to Hide Credential Theft



ThreatFabric has disclosed Bazuka, a previously unknown Android malware framework with LLM integration for managing victims at scale. It was found in late October 2026 during an NFC-relay banking Trojan investigation.

- Bazuka is a previously unknown Android malware framework, not a single-purpose Trojan.
- It offers large language model (LLM) integration for victim management and control at scale.
- The headline reports fake screen overlays used to hide credential theft and device control.
- ThreatFabric, a Dutch mobile security firm, found it in late October 2026.
- The discovery came during an investigation into an NFC-relay banking Trojan.

Researchers at ThreatFabric, a Dutch mobile security company, have described a previously unknown Android malware framework named Bazuka. The company says it found the threat in late October 2026 while investigating an NFC-relay banking Trojan.

What has been reported

Bazuka is described as a full malware framework rather than a single tool. Its notable feature is integration with large language models (LLMs), which is intended to help operators manage and control victims at scale. According to the headline, it relies on fake screen overlays to conceal credential theft and control of the device.

The source excerpt is brief, so details such as distribution method, targeted institutions or regions, and technical indicators are not available here.

Why it matters

Financial institutions and their customers rely heavily on mobile channels. A framework that hides its activity behind overlays can make theft of credentials harder for users to notice, and its link to an NFC-relay banking Trojan investigation points to the banking context.

This is a reason for calm review, not alarm. Teams should read the full ThreatFabric findings when available, and check whether existing mobile fraud and endpoint controls cover overlay-based abuse.

What to do now

1. Obtain the full ThreatFabric report and extract any indicators of compromise for your threat-monitoring tooling.
2. Review whether your mobile banking app and fraud systems detect overlay attacks and abnormal device-control behaviour.
3. Remind customers and staff to install apps only from official stores and to be wary of unexpected permission requests, especially accessibility access.
4. Check that managed corporate Android devices are enrolled in MDM with app-install restrictions.
5. Confirm your fraud and incident response playbooks cover mobile malware and credential theft scenarios.