Bazuka Android Malware Framework Disclosed, Using Fake Overlays and LLM Integration



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.
- It offers large language model (LLM) integration for managing and controlling victims at scale.
- ThreatFabric, a Dutch mobile security company, found it in late October 2026.
- The discovery came during an investigation into an NFC-relay banking Trojan.
- The report's headline links it to fake screen overlays used to hide credential theft and device control.

Researchers at ThreatFabric, a Dutch mobile security company, have described a previously unknown Android malware framework named **Bazuka**. According to the report, it includes large language model (LLM) integration intended to help operators manage and control victims at scale.

What was reported

ThreatFabric says it found the threat in late October 2026 while investigating an NFC-relay banking Trojan. The company characterises Bazuka as a full malware framework rather than a single-purpose tool. The report's headline indicates that it uses fake screen overlays to conceal credential theft and device control from the user.

The excerpt available to us does not set out distribution methods, targeted countries or institutions, or technical indicators. We have therefore not assumed any impact on Saudi organisations.

Why it matters

Malware that pairs overlay-based deception with centralised management of many infected devices raises the risk for mobile banking and workforce apps. Institutions that serve customers through Android apps, or allow staff to reach corporate systems from mobile devices, should treat this as a prompt to review their mobile defences.

The practical response is review, not alarm. Check what your mobile fraud and endpoint controls can detect, confirm that your teams can act quickly on indicators once ThreatFabric or others publish them, and remind customers and staff of basic safe-installation habits.

What to do now

1. Review your threat-intelligence feeds for Bazuka indicators published by ThreatFabric and add them to detection once available.
2. Check whether your mobile banking apps can detect screen overlays and risky accessibility or device-control behaviour.
3. Confirm that mobile device management enforces app installation only from approved sources on corporate Android devices.
4. Test fraud-monitoring rules for suspicious sessions that follow credential entry on newly compromised devices.
5. Send customers and staff a short reminder not to install apps from outside official stores or grant unexpected device permissions.