

Forum:[Hack Forums](#)

Thread: [\[Android\] What is the best way to obfuscate apk](#)

baraaelgamal - August 1, 2025, 4:14 am

I need a way to obfuscate my apk trojan cuz I am trying old ways but they seem to not work anymore

DramaKing - August 1, 2025, 10:17 am

(Aug 1, 2025 04:14 AM)baraaelgamal Wrote: [\[CITE\]](#) I need a way to obfuscate my apk trojan cuz I am trying old ways but they seem to not work anymore
They don't. APK crypters are dead.

???????????? - August 2, 2025, 7:21 am

(Aug 1, 2025 04:14 AM)baraaelgamal Wrote: [\[CITE\]](#) I need a way to obfuscate my apk trojan cuz I am trying old ways but they seem to not work anymore

1. Dynamic Code Loading

- Alert on use of `DexClassLoader` / `PathClassLoader` loading from writable storage.

- Alert on heavy use of reflection (`java.lang.reflect.*`) especially when followed by other suspicious activity. Detect `System.loadLibrary` calls with unexpected/native libraries.

- Flag runtime downloads of `.dex`/`.jar` files into app data and immediate execution. Correlate dynamic loading events with subsequent outbound network activity (C2-style beaconing).

- Maintain a whitelist of known legitimate apps/frameworks to reduce false positives.

2. Unexpected Network Traffic / Beaconing

- Detect periodic outbound connections with consistent intervals (e.g., 50–70 seconds) to external endpoints.

- Flag connections to newly seen or low-reputation domains/IPs. Identify small, regular “heartbeat” payloads (consistent size/frequency).

- Measure entropy of request bodies or DNS query names; high entropy can indicate encoded C2 traffic. Spot DNS anomalies: repeated failed lookups followed by success, or rapidly generated similar-looking domains (possible DGA).

- Combine with preceding suspicious behavior (e.g., dynamic code loading) to raise confidence.

3. Hidden VPN / Tunnel Usage

- Alert when non-approved processes create or bring up `tun*` / `tap*` interfaces.

- Detect execution of tunneling binaries (e.g., `openvpn`, `wireguard`, `stunnel`) outside of expected/approved clients. Identify long-lived encrypted sessions to uncommon ports with low variance in packet size (possible encapsulation).

- Look for TTL or MTU anomalies inconsistent with baseline traffic (signs of tunneling). Detect nested protocols or encapsulated traffic patterns (e.g., unexpected protocol headers inside others).

- Monitor processes binding to unexpected network interfaces or creating virtual adapters.

Correlation & Response

- Combine multiple signals (e.g., dynamic loading + beaconing + tunnel creation) before escalating. Enrich destinations with reputation data. Set thresholds to avoid alert fatigue (require multiple beacons, persistence, or chaining).

- On detection: isolate the host, capture memory/network traces, and begin investigation using the chained indicators.

Chornaya Magiya - August 2, 2025, 7:23 am

(Aug 1, 2025 04:14 AM)baraaelgamal Wrote: [\[CITE\]](#) I need a way to obfuscate my apk trojan cuz I am trying old ways but they seem to not work anymore

Create .apk which can dynamically read code from your server if specified args is met.

Mia_K5236 - August 2, 2025, 2:09 pm

(Aug 2, 2025 07:23 AM)Chornaya Magiya Wrote: [\[CITE\]](#) Create .apk which can dynamically read code from your server if specified args is met.

This is the best way here imo. Side load it from a hosted server.

rebeecer - August 4, 2025, 6:29 am

Which RAT do you use?