App Analysis Checklist:

1. **App Name:** MyJPJ

2. **Date of Analysis**
    a. **Static Analysis Date (Exodus Privacy / MobSF):** July 3 - July 4, 2025
    b. **Dynamic Analysis Date (Network Traffic Analysis):** July 2, 2025

File Analyzed:

3. **APK Version Analyzed:** 3.0.1

4. **PCAP Version Analyzed:** 3.0.1

5. **Screenshots:** MyJPJ Screenshots

Application Description:

6. **Type:** Official government app

7. **Cost (Free, Freemium, Paid):** Free

8. **Play Store Link:** https://play.google.com/store/apps/details?id=com.jpj.jpj_info

9. **Number of Downloads:** 10M+

10. **Last Updated Date (on Play Store):** July 21, 2025

11. **Version on Play Store (at time of analysis):** 3.0.1

12. **Developer Name:** Jabatan Pengangkutan Jalan, Malaysia

13. **App Signature:** Google Inc. (Android)

14. **Contact Email:** mobileapps@jpj.gov.my

15. **Terms of Use / Privacy Policy Link:**
    a. I found it in the app, but it is in Malay. Here's the screenshot:
    MyJPJ Privacy Policy.jpeg

16. **Play Store Description:**

Maklumat Jabatan Pengangkutan Jalan (JPJ) boleh diperolehi melalui Aplikasi Mobile dengan lebih mudah diakses dan cepat. Pengguna juga boleh mendapatkan perkhidmatan percuma seperti semakan saman.

MyJPJ mengandungi:
- Lokasi JPJ Negeri dan Cawangan di seluruh Malaysia.
- Perkhidmatan Atas Talian seperti semakan saman, senarai hitam, maklumat lesen memandu dan pertanyaan nombor pendaftaran kenderaan terkini.

Kelebihan MyJPJ:
- Kebolehcapaian untuk platform Android Dan iOS.
- Paparan yang lebih jelas dan mesra penggunaan
- GPS Lokasi pejabat JPJ, UTC,cawangan.
- Tujuh (7) perkhidmatan percuma
- Link mudah ke portal dan sistem JPJ

MyJPJ contains:
- RTD State and Branches All Over Malaysia location online services such as summons enquiry, blacklist, driver's license information and List of latest vehicle registration numbers.

The advantages:
-Clear, user-friendly display
- GPS Location of JPJ office, UTC, branch.
- Seven (7) free services
- Easy links to JPJ portals and systems

[Minimum supported app version: 3.0.0]

Trackers (from Exodus):

17. **List of Identified Trackers + Category:**

Tracker	Category
Huawei Mobile Services (HMS) Core	Location, Advertisement, Analytics
OneSignal	Notifications

18. **Link to Exodus Privacy report**

Related Companies and Services:

19. **Companies connected to app function:**
    - **Google / Alphabet:** Provides essential infrastructure for app functionality, including Google Play Store, APIs, and backend services.
    - **MaxCDN (BootstrapCDN):** Supplies web libraries, fonts, and other assets for improved loading speed.
    - **Cloudflare:** Delivers CDN and security solutions for fast and secure content delivery.
    - **TM Technology Services Sdn. Bhd.:** Supports local hosting and connectivity.
    - **Huawei Mobile Services (HMS) Core:** Enables integration and device-specific features for Huawei users.
    - **OneSignal:** Powers push notifications and in-app messaging.

20. **Third-party service providers for payments, identification, and social media:** MyJPJ does not use any third-party providers for payment processing, identity verification, or social media integration.

Permissions:

21. **Number of Permissions:**
    - **According to the Playstore:** 13 distinct permissions.
    - **According to Exodus Privacy:** 35 permissions.
    - **According to usage test:** 2 permissions that are explicitly requested.

22. **Permissions according to Exodus Privacy:**
    - ACCESS_NETWORK_STATE *view network connections*
    - 🎥 ❗ CAMERA *take pictures and videos*
    - FOREGROUND_SERVICE *run foreground service*
    - GET_TASKS *retrieve running apps*
    - INTERNET *have full network access*
    - PACKAGE_USAGE_STATS
    - POST_NOTIFICATIONS
    - READ_APP_BADGE
    - 📁 ❗ READ_EXTERNAL_STORAGE *read the contents of your shared storage*
    - READ_MEDIA_IMAGES
    - READ_MEDIA_VIDEO
    - RECEIVE_BOOT_COMPLETED *run at startup*
    - 💓 USE_BIOMETRIC *use biometric hardware*
    - 💓 USE_FINGERPRINT *use fingerprint hardware*
    - VIBRATE *control vibration*
    - WAKE_LOCK *prevent phone from sleeping*

- 📁 ❗ WRITE_EXTERNAL_STORAGE *modify or delete the contents of your shared storage*
- UPDATE_COUNT
- RECEIVE
- READ_SETTINGS
- UPDATE_SHORTCUT
- CHANGE_BADGE
- READ_SETTINGS
- ❗ WRITE_SETTINGS
- DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION
- C2D_MESSAGE
- UPDATE_BADGE
- READ_SETTINGS
- ❗ WRITE_SETTINGS
- READ
- WRITE
- BROADCAST_BADGE
- PROVIDER_INSERT_BADGE
- BADGE_COUNT_READ
- BADGE_COUNT_WRITE

The icon ❗ indicates a 'Dangerous' or 'Special' level according to Google's protection levels.

23. **Permissions requested during actual use:**
    - 🔵 Camera
    - 🔵 Files and media
    - 🔵 Notifications

    🔴 This icon indicates a required permission.
    🔵 This icon indicates an optional permission, but some functionality might be lost if not granted.

Data:

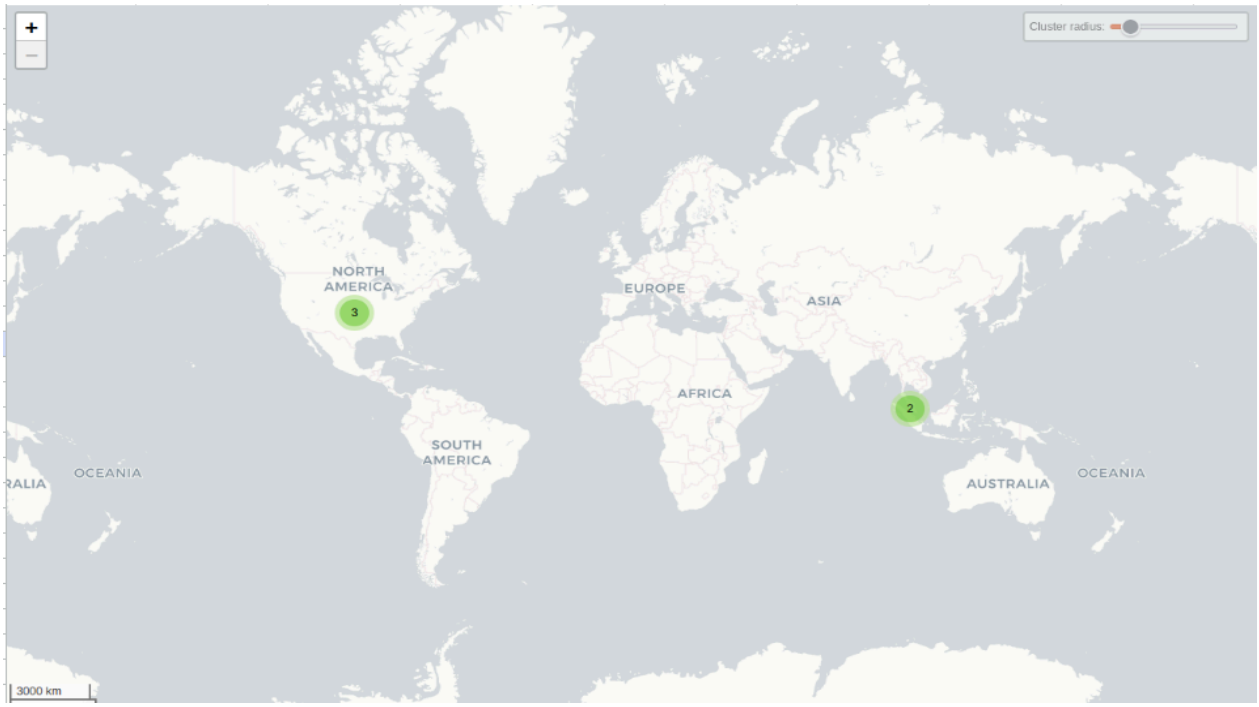
24. **Data requested from the user during the use of the application:**
    - 🔴 Malaysian Identification Card Number
    - 🔴 Name
    - 🔴 Email
    - 🔵 Biometric authentication (optional, for sign-in)
    - 🔴 Vehicle registration number (used for vehicle license inquiry and renewal, and for checking traffic summons; the summons payment feature could not be tested during the analysis period)

🔴 This icon indicates that this information is required.
🔵 This icon indicates that this information is optional.

25. **Table of connections made:**

Address	Packets	Country	City	AS Number	AS Organization
8.8.8.8	30	United States		15169	GOOGLE
10.1.10.1	9785				Bogon IP
104.18.11.207	22			13335	CLOUDFLARENET
110.159.245.15	7449	Malaysia	Bandar Puncak Alam	4788	TM TECHNOLOGY SERVICES SDN. BHD.
110.159.245.18	538	Malaysia	Bandar Puncak Alam	4788	TM TECHNOLOGY SERVICES SDN. BHD.
172.217.25.78	1053	United States		15169	GOOGLE
216.58.199.238	693	United States		15169	GOOGLE

26. **Map:**



Data Collection and Sharing:

27. **Data shared with third parties according to Play Store:** The developer says this app doesn't share user data with other companies or organizations.

28. **Data collected and used according to Play Store:** The developer says this app doesn't collect user data.

    We remind you that anonymized or de-identified data is not required to be disclosed as shared with third parties under Google's policy. However, such data may still be collected or processed, and our privacy practices do not guarantee that anonymization is irreversible or prevents future linking to personal identities.

29. **Security practices according to Play Store:**
    - Data is encrypted in transit
    - You can request that data be deleted

30. **Data collected and used according to Privacy Policy:**

Data Type	Use / Purpose
Device information (model, OS, phone number, service provider, IMEI, location)	Service delivery, troubleshooting, analytics, and security
Name and contact number	User identification, account management
Email address	Communication, notifications, account recovery
Transactional/service usage data	Process payments, manage features, improve user experience

According to the privacy policy, the app may collect the following types of personal information to provide and improve its services:The privacy policy states that data may be used for:

- Delivering app services and features
- Improving user experience
- Ensuring security and preventing fraud
- Fulfilling legal obligations
- Communicating with users (e.g., updates, inquiries)
- Service analysis, troubleshooting, and marketing (some data may be shared with third parties for these purposes)

Data sharing:
Data may be shared with third-party service providers or government agencies for payment processing, analytics, fraud prevention, or as required by law.

Security:
The privacy policy indicates that reasonable measures are taken to protect user data. However, users are advised to be cautious when clicking on external links.

Notable Issues:

31. **Important notes or red flags for user consideration (if any):**
    No significant issues or red flags were identified during this review. The app appears to follow standard security and privacy practices, but users are still encouraged to review app permissions and privacy settings regularly.

Conclusion:

Overall, the MyJPJ app demonstrates standard behavior for a government utility app, with no signs of suspicious network activity or connections to unknown domains. All connections observed during testing were to reputable services, such as Google, Cloudflare, and Malaysian government servers.

The app requests a broad range of permissions, including some that could be considered sensitive, such as access to the camera, storage, and system settings. While most of these are common for apps with similar functionality, users should remain mindful of the potential risks, especially on older or unpatched Android devices.

Two trackers were detected: Huawei Mobile Services (HMS) Core and OneSignal. HMS Core is commonly used for device integration, analytics, and advertising, raising privacy considerations, especially for users concerned about data sharing with third parties. OneSignal is used for push notifications and basic analytics. Both trackers are widely used, but users should be aware of their presence and the potential for data collection beyond basic app functionality.

No critical security issues were identified during the analysis, and the app uses encrypted connections for communication. However, some outdated cryptographic practices, exported components, and support for legacy Android versions present moderate risks.

Recommendation:

For most users, MyJPJ is safe to use as intended, provided that device software is kept up to date and permissions are reviewed regularly. Privacy-conscious users should be aware of the app's data access and tracking behavior. Developers are encouraged to further improve data protection practices, minimize unnecessary permissions, and ensure all components are properly secured.