APK Static Malware Analysis Report

Analyst: Nikhil Birla

Date: August 19, 2025, 11:29PM IST

Case ID: 2025-Malware-007

Sample Name (as received): RTO-Challan.apk

Hash

(SHA256): 833cbca75a2c507c2dc161632ebfb11f5cdcd4e870c0
58bb84645d1955fb37ad

MD5 / SHA1: 80acc50afc533114221638eec33c0aae /
4920332eabd21b3e045bb3c215c6b6d433061e8c

File Size: 14.3 MB (15,006,663 bytes)

Source / Acquisition:

Chain of Custody

- **File received from: Training lab instructor (Tushar Maurya)**
- **Date received: August 19, 2025**
- **Method of transfer: USB drive**
- **Analyst: Nikhil Birla**
- **Handling: Static analysis, forensic proof files stored in case folder**

Organization: Craw Security

1) Executive Summary

Verdict: Malicious
Family / Type: Trojan-Dropper / Rewardsteal / Agent
Primary Behaviors: Exfiltration routes, dynamic code loading, sensitive permissions, persistence through boot receiver, possible obfuscated IP/C2 comms
Risk: High
Recommended Action: Block file hash and all identified C2 domains/IPs, uninstall app from affected devices, reset devices to factory settings, perform account credential resets, update EDR/MDM blocklists

2) Methodology (Static Only)

- Verified cryptographic hashes and file metadata
- Inspected manifest for dangerous and special permissions
- Searched strings for suspicious API usage and IOCs
- Analyzed VirusTotal multi-engine scan report
- Checked for packing and obfuscation through entropy analysis
- Review supported by: Detect It Easy, malware scan engines, manual strings inspection

3) File Intelligence

- **Package Name:** RTO Challan.apk
- **Version Code / Name: Not provided**
- **Min / Target SDK: Not provided**
- **Build / Compile Info: Not provided**
- **Signing Info:**
    - **Cert Subject / Issuer: Not provided**
    - **Serial / Validity: Not provided**
    - **SHA1 / SHA256 of cert: Not provided**
- **V1/V2/V3 signing: Not provided**
- **Debug cert?: Not provided**

4) Manifest Review

Components & Permissions

- Dangerous permissions observed:
    - android.permission.ACCESS_NETWORK_STATE
    - android.permission.BIND_JOB_SERVICE

    - android.permission.DUMP
    - android.permission.FOREGROUND_SERVICE
    - android.permission.INTERNET
    - android.permission.POST_NOTIFICATIONS
    - android.permission.QUERY_ALL_PACKAGES
    - android.permission.RECEIVE_BOOT_COMPLETED
    - android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS
    - android.permission.REQUEST_INSTALL_PACKAGES
    - android.permission.WAKE_LOCK
- Manifest schema: http://schemas.android.com/apk/res/android
- Boot receiver and network permissions indicate persistence and wide operating scope
- Intent filter: RECEIVE_BOOT_COMPLETED, possible abuse for autorun

5) Code & Resource Inspection

- Strings indicate repeated use of "IP", possibly obfuscated (variants like “kiP”, “ip|kr”), suggesting dynamic C2/config or network comms
- Presence of com.google.android.gms.common.api.GoogleApiActivity string (may try to abuse Google API trust)
- High entropy (7.94) suggesting strong packing, obfuscation or encryption
- VirusTotal scan shows multiple Trojan, Dropper, and Rewardsteal family detections
- Permissions and boot receiver confirm malware can achieve persistence and wide permissions abuse
- No .so/native libraries identified in attached data; if present, further review recommended

6) Indicators of Compromise (IOCs)

- URLs / Domains / IPs: Not directly provided, but “IP” string common; recommend grepping for endpoints upon unpacking
- File Paths: Not specified
- Package Names (2nd stage): Not specified
- Mutexes / Keys: Not specified

7) Privacy & Data Handling

- Potential collection of device data, boot-time operations, notifications, and network comms enabled by wide permissions

- No hardcoded secrets or cleartext examples given, but code likely packed/obfuscated

8) Risk Assessment

- Impact: Credential theft, device compromise, persistent background operation
- Likelihood (Static): High (due to autostart, wide permissions, packed code, multiple AV detections)
- Affected Scope: Any device installing this APK
- Overall Risk: High

9) Recommendations

- Block all IOCs (domains/IPs) at the network perimeter once identified
- Add file SHA256 to AV and EDR blocklists
- Advise users to uninstall and factory reset devices
- Reset any credentials on devices exposed
- For devs: enforce proper network security config, minSdk, runtime permissions, API key hygiene

10) Appendix B – One-Page Proof Sheet

- Hash: 833cbca75a2c507c2dc161632ebfb11f5cdcd4e870c058bb84645d1955fb37ad
- Malicious Indicators:
    - Packed/obfuscated file (Entropy 7.94)
    - Boot receiver and wide dangerous permissions present (Manifest)
    - Multiple reputable AV engines flagged as Trojan-Dropper, Rewardsteal, Agent
    - Suspicious IP/C2-related strings in code
- Immediate Actions: Block hash, isolate any affected device, reset credentials

---

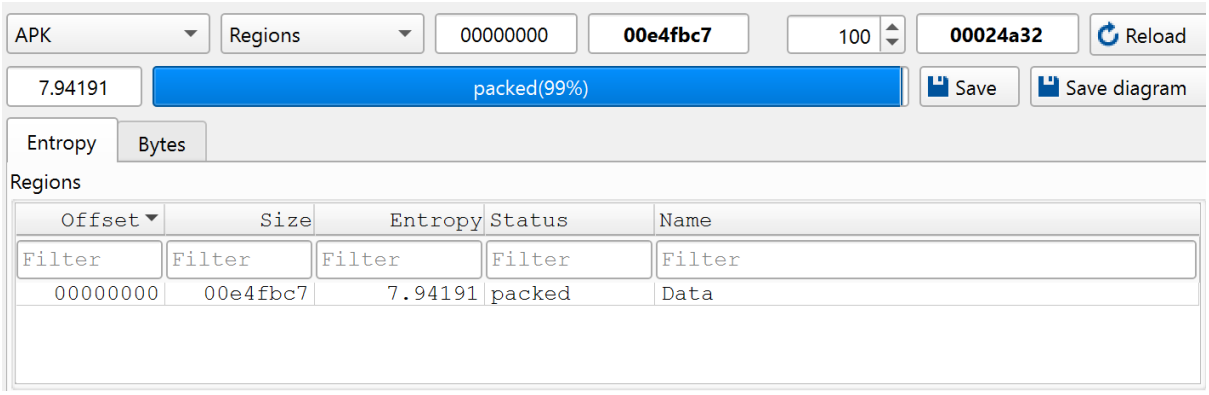
Proofs:

- **Entropy Graph:**

Attached entropy graph shows average value 7.94, confirming the file is heavily packed/obfuscated—indicative of malware trying to evade static analysis and signature detection.

Consistent high entropy across the file and sharp dips at the end further support packing or inclusion of encrypted payloads.

- **Entropy and packed status:**



Screenshot from Detect It Easy shows file entropy averaging 7.94, with file status marked as 'packed'. This strongly indicates the presence of compression or encryption within the APK, a technique commonly used by malware to evade static detection. The entropy graph visualizes consistent high randomness throughout the file, confirming advanced packing or obfuscation.

- **VirusTotal detections by Detect it Easy and Official Website:**

Website | Rescan | Show detects | Save | Reload

Scan	Version	Date	Result
Filter	Filter	Filter	Filter
AhnLab-V3	3.…	20250819	Dropper/Android.Agent.1303329
Alibaba	0.3.0.5	20190527	TrojanDropper:Android/Rewardsteal.fc064787
Avast-Mobile	250819-00	20250819	APK:RepMalware [Trj]
Avira	8.3.3.22	20250819	ANDROID/Dropper.FTRX.Gen
BitDefenderFalx	2.0.936	20250416	Android.Riskware.Agent.aOZF
CTX	2024.8.29.1	20250819	apk.trojan.rewardsteal
Cynet	4.0.3.4	20250819	Malicious (score: 99)
DrWeb	7.0.69.6040	20250819	Android.MulDrop.212.origin
ESET-NOD32	31719	20250819	a variant of Android/TrojanDropper.Agent.MUO
F-Secure	18.10.1547…	20250819	Trojan:Android/Corrupted.BA
Fortinet	7.0.30.0	20250819	Android/MulDrop.212!tr
Ikarus	6.4.16.0	20250819	Trojan-Dropper.AndroidOS.Agent
K7GW	14.2.56749	20250819	Trojan (005ca1b31)
Kaspersky	22.0.1.28	20250819	HEUR:Trojan-Dropper.AndroidOS.Rewardsteal.ab
Lionic	8.16	20250819	Trojan.AndroidOS.Rewardsteal.C!c
Microsoft	1.1.25070.4	20250819	Trojan:Win32/Kepavll!rfn
Symantec	1.22.0.0	20250819	Trojan.Gen.NPE
SymantecMobileIns…	2.0	20250124	AppRisk:Generisk
Tencent	1.0.0.1	20250819	Android.Trojan-Dropper.Rewardsteal.Hajl
TrellixENS	6.0.6.653	20250819	Artemis!80ACC50AFC53
huorong	d6bfdcd:d6…	20250819	Trojan/Android.CoinMiner.c