TraceX Labs Security Advisory on Fake 'Cockroach Janta Party' Android Malware Spreading Through WhatsApp and Telegram

TraceX Labs warns Android users about a fake “Cockroach Janta Party” APK spreading through WhatsApp and Telegram that may steal sensitive data.

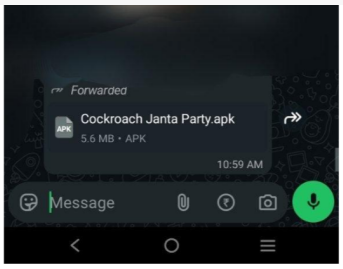


Figure 1: Screenshot showing the fake "Cockroach Janta Party.apk" (~5 MB) being shared via a WhatsApp chat or channel. The social engineering lure references the GenZ political party to trick supporters into downloading the malicious file. Note the APK icon and file size visible in the chat.

Cockroach Janta Party” APK spreading through WhatsApp & Telegram - TraceX Labs Report

NEW YORK, TX, UNITED STATES, May 24, 2026 /EINPresswire.com/ -- Indian cybersecurity and threat intelligence company TraceX Labs has issued a public security advisory warning Android users about a fake “Cockroach Janta Party” mobile application that is reportedly spreading through WhatsApp, Telegram groups, invite links, and third-party APK download websites.

According to the cybersecurity researchers, the application is disguised as a political-themed Android APK and is being circulated online using the name “Cockroach Janta Party.apk.” Researchers say the malware campaign appears to target Android users searching for “Cockroach Janta Party APK,” “CJP app,” and other related viral political content online.

> Cybercriminals are increasingly using viral online trends and fake APK files to target Android users through messaging platforms.”
>
> *Editorial Desk*

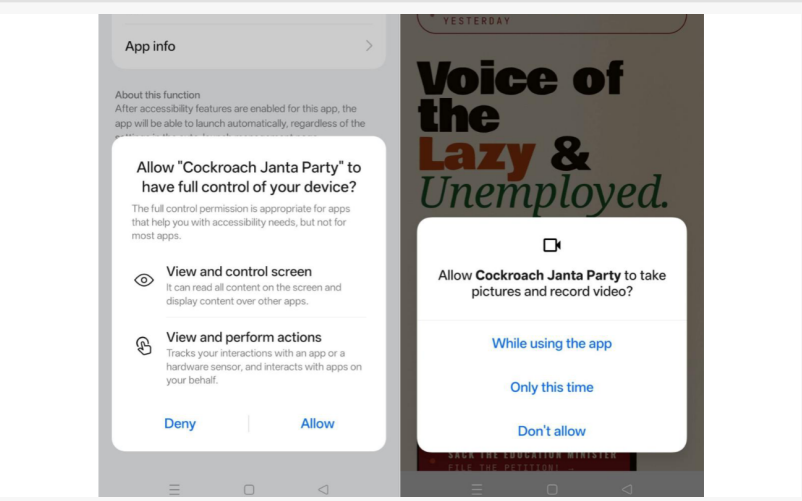
TraceX Labs stated that the fake application is designed to trick users into manually installing the APK outside official app marketplaces such as the Google Play Store. The company warned that attackers are using social engineering tactics, viral internet discussions, and trending political conversations to gain user trust and encourage downloads through messaging platforms and malicious websites.

The cybersecurity advisory clarified that the legitimate Cockroach Janta Party movement is not associated with the malware campaign and is itself a victim of impersonation by cybercriminals

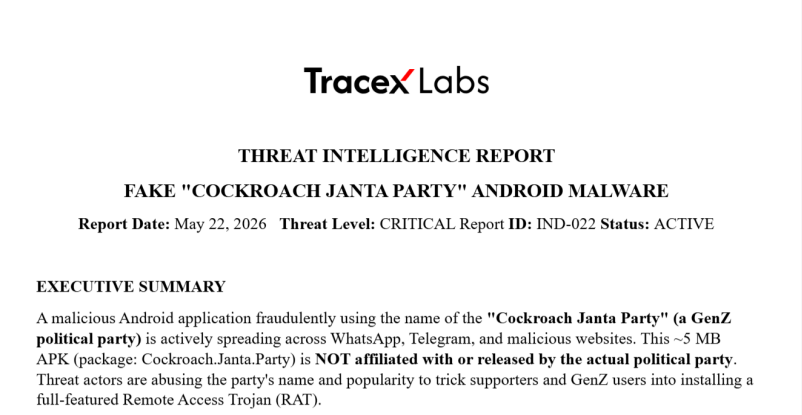
misusing the movement's name and online popularity.

According to the published threat intelligence report, the malicious APK may collect sensitive information stored on infected Android devices, including SMS messages, OTPs, contacts, call history, photos, documents, and other device-related information. Researchers also stated that the spyware can potentially monitor activity in the background and attempt to access authentication-related information used for banking and online accounts.

During the investigation, TraceX Labs researchers identified multiple dangerous Android permissions requested by the application after installation. These reportedly include SMS access, contact access, storage permissions, camera permissions, call log access, and Accessibility Service permissions.



Cockroach Janta Party" Apk Takes Accessibility permissions for Remote Access - TraceX Labs Report



TraceX Labs

THREAT INTELLIGENCE REPORT

FAKE "COCKROACH JANTA PARTY" ANDROID MALWARE

Report Date: May 22, 2026 **Threat Level:** CRITICAL Report **ID:** IND-022 **Status:** ACTIVE

EXECUTIVE SUMMARY

A malicious Android application fraudulently using the name of the **"Cockroach Janta Party" (a GenZ political party)** is actively spreading across WhatsApp, Telegram, and malicious websites. This ~5 MB APK (package: Cockroach.Janta.Party) is **NOT affiliated with or released by the actual political party**. Threat actors are abusing the party's name and popularity to trick supporters and GenZ users into installing a full-featured Remote Access Trojan (RAT).

"Cockroach Janta Party" - TraceX Labs Report

Security experts warned that Accessibility permissions should be granted carefully because they can allow applications to monitor screen activity and interact with device functions in the background. According to the advisory, cybercriminals increasingly abuse such permissions in Android malware campaigns targeting mobile users.

Researchers also found that the malware uses Telegram-based infrastructure as part of its communication mechanism. According to TraceX Labs, using common messaging infrastructure can make suspicious traffic appear similar to normal application traffic during routine monitoring.

The report further suggests that Indian Android users may be among the primary targets of the campaign. Researchers reportedly identified references related to India and Reliance Jio within parts of the malware codebase during their analysis.

"The fake APK is designed to misuse public interest and viral online discussions to target Android users through social engineering tactics," said Santhosh Kumar, cybersecurity researcher

associated with the investigation. “Users should avoid downloading APK files from unknown sources and remain cautious while installing apps shared through messaging platforms.”

TraceX Labs advised Android users to install applications only from trusted sources such as the Google Play Store and avoid APK files shared through WhatsApp, Telegram, or unfamiliar websites. The company also recommended keeping Google Play Protect enabled, reviewing app permissions carefully, avoiding Accessibility access for unknown applications, and using authenticator apps instead of SMS-based OTP authentication whenever possible.

Users who suspect that they may have installed a suspicious APK are advised to uninstall the application immediately, review Accessibility permissions, reset passwords using another trusted device, and monitor important accounts for unusual activity.

The complete threat intelligence report released by TraceX Labs includes malware analysis findings, Android permission analysis, network indicators, reverse engineering observations, YARA detection rules, and security recommendations for users and organizations.

Threat Report PDF:
Cockroach Janta Party Malware Threat Report 2026 PDF

Web Report Version:
Threat Intelligence Report Web Version

About TraceX Labs

TraceX Labs is an Indian cybersecurity and threat intelligence organization focused on malware analysis, cyber threat investigations, Android security research, digital risk monitoring, phishing infrastructure analysis, OSINT, and incident response intelligence. The organization regularly publishes public security advisories and technical reports related to emerging cyber threats and online fraud campaigns.

Editorial Desk
Editorial Desk
email us here