PRESS RELEASE

WEST DISTRICT

Date 21/11/2026

INTER-STATE OPERATION IN JAMTARA (JHARKHAND) & ADJOINING STATES UP, WEST BENGAL AND BIHAR)

22 TOP CYBER CRIME SCAMSTERS SYNDICATE WITH PANEL & APK FILE DEVELOPERS WERE ARRESTED FROM JAMTARA (JHARKHAND) THE CYBER CRIME HOTSPOT AND ADJOINING STATES.

5 DAYS OPERATION WITH SEVEN POLICE TEAMS CONSISTING OF 64 POLICE PERSONNEL CONDUCTED RAID AT 17 PLACES VIZ BIRAJPUR, KARMATAR, MARGOMUNDA, SARWAN, NARAINPUR, SARATH, MURLI PAHARI, DHUMARIA, PARTOL, GIRIDIH, PATHROL, NAUADI, NAGADARI, FATEHPUR, CHAKAI, JAMUI & NALANDA, ASSANSOLE, KOLKATA AND GORAKHPUR

TOTAL FRAUD COMMITTED BY THESE SYNDICATE IS MORE THAN 20 CRORE TARGETING 22,139 VICTIMS ACROSS THE COUNTRY. TOTAL 2080 NCRP COMPLAINTS ARE DIRCETLY CONNECTED WITH THE ARRESTED PERSONS

MORE THAN 1300 NCRP COMPLAINTS RELATED TO APK FILES EXAMINED, 32 MALICIOUS APK FILES FORENSICALLY EXAMINED AND 56 TELEGRAM PROFILES CONNECTING TO THIS MODUS OPERANDI INVESTIGATED.

63 OFFENDING MOBILE PHONES USING APK PANEL FILES, 2 LAPTOPS, 2 MACKBOOK AND 1 TAB RECOVERED FROM THE CRIMINALS.

IMPACT OF THE OPERATION – MORE THAN 50% REDUCTION OF THE COMPLAINTS RELATED APK FILE FRAUD DURING LAST 10 DAYS SINCE THIS OPERATION IN DELHI (FROM 2 TO 10 NOVEMBER NCRP COMPLAINTS RELATED TO APK FRAUD- 1406 & FROM 11 TO 17 NOVEMBER APK FRAUD- 724)

THE ACCUSED PERSONS EXPLOITED SOCIAL MEDIA PLATFORMS AND MESSAGING APPLICATIONS TO LURE VICTIMS, OBTAIN THEIR PERSONAL AND BANKING DETAILS AND COMMIT CYBER FRAUD.

MODUS OPERANDI – MALICIOUS APK- PANEL BASED CYBER FRAUD

Over the past three months, more than 1,000 complaints relating to bank account takeovers and cyber fraud through malicious APK files were identified during the analysis of NCRP data. The fraudsters primarily targeted senior citizens by impersonating bank officials and offering assistance in Life Certificate verification, KYC updation, credit card issuance, BSES and IGL connection and enhancement of credit limits etc.

During interaction with victims, it emerged that the accused contacted them through WhatsApp and induced them to download malicious APK files under the pretext of completing banking-related verification or updation procedures. Once installed, these applications displayed fake banking forms and sought access to sensitive information, including personal details, banking credentials, SMS, OTPs, calls and gallery contents.

By exploiting the permissions granted by victims, the fraudsters gained unauthorised access to their mobile devices and confidential financial information, enabling them to take over bank accounts, conduct fraudulent transactions, siphon off funds and utilise available credit card limits without the victims' knowledge.

INETR-STATE OPERATION – SIX PHASES OF THE OPERATION

1. Preparation & Strategic Planning

Intelligence development, target identification and operational planning.

- Analysis of more than **1,000 NCRP** complaints relating to APK fraud and bank account takeover.
- Analysis of more than **20 e-FIRs** involving similar modus operandi.
- Forensic examination and decoding of **32 malicious APK files**.
- Analysis of more than **56 suspected Telegram profiles** and associated WhatsApp numbers.
- Identification of the alleged **APK developers**, distributors and sub-distributors.
- Identification of target locations across **Jamtara, Deoghar, Giridih, Jamui and adjoining areas, including Kolkata.**

- Constitution of seven specialised police teams comprising 64 police personnel under the supervision of SHO/Cyber Insp Vikas kumar Buldak, overall supervision of ACP/Ops Sh. Rajesh Kumar and under the guidance of worthy DCP/West Sh. Hareshwar V. Swami.

2. Journey & Mobilisation

Logistical planning and coordinated movement of the entire police force from Delhi to the operational area.

- Coordinated movement of **64 police personnel** with necessary logistical arrangements.
- Arrival at the operational base and preparation for deployment across different target locations.
- Ensuring that all seven teams remained organised and ready for immediate operational deployment.

3. Ground-Level Preparation & Recce

Converting digital intelligence into physical identification of suspects and locations.

- Detailed ground-level reconnaissance of identified villages and suspected locations.
- Physical verification of addresses and identification of the accused persons.
- Mapping of remote villages, narrow roads, open fields and difficult approaches.
- Identification of possible escape routes and surrounding geographical features.
- Collection of local intelligence and verification of the presence and movement of suspects.
- Correlation of digital intelligence, technical leads and geographical mapping with ground-level findings.
- Multiple rounds of recce to ensure accurate identification of targets before execution.

4. Plan Execution – Coordinated Interstate Raids

Simultaneous and continuous execution of the operational strategy.

- Execution of the pre-planned raid strategy by seven specialised teams.
- Continuous raids conducted from **11 November to 15 November 2026**.
- Deployment of teams across multiple locations in **Birajpur, Karmatar, Margomunda, Sarwan, Narainpur, Sarath, Murli Pahari, Dhumaria, Partol,**

Giridih, Pathrol, Nauadi, Nagadari, Fatehpur, Chakai(Jamui), Assansole And Kolkata

- Real-time sharing of intelligence and immediate redeployment whenever fresh leads emerged.
- Handling of difficult terrain, local resistance and attempts by accused persons to escape.
- Pursuit and apprehension of suspects, including those who attempted to flee through open fields.

5. Co-Ordination and co-operation

The entire operation was carried out in close coordination with Jharkhand and Bihar Police.

6. Arrests, Recoveries & Digital Evidence Collection

Breaking the operational chain of the cyber fraud syndicate.

- Successful arrest **of 22 accused persons belonging to 11 identified scamster** groups and the alleged APK panel development network.
- Apprehension of the alleged developers of the malicious APK-generation infrastructure.
- Recovery of **63 mobile phones, two laptops, two MacBooks and one tablet**.
- Recovery of electronic devices containing incriminating digital evidence relating to malicious APK files and the fraud network.
- Identification of linkages between developers, distributors, sub-distributors and operational fraudsters.
- Development of further leads for identifying other associates and connected cyber fraud networks.

DETAILS OF ARRESTED PERSONS

S. No.	Name of accused	District	Total
1.	Jafir Ansari	Jamtara	08
2.	Md. Azhar Ansari	__	
3.	Ahamed Razza	__	
4.	Amir Hamja	__	
5.	Md. Asif	__	
6.	Ajay Kumar Mandal	__	
7.	Mukesh Mandal	__	
8.	Pawan Kumar Mandal	__	
9.	Manjoor Ansari	Deoghar	04
10.	Maniruddin Ansari	__	

11.	Md Ajamul Ansari	__	
12.	Niraj Kumar Dass	__	
13.	Jiblal Mandal	Giridih	02
14.	Sonu Kumar Verma	__	
15.	Rahul Mandal	Dumka	01
16.	Tarjan Bharti R	Jamui	04
17.	Vikram Boss	__	
18.	Jaynandan Das @ RAVAN	ASANSOLE	
19.	Bikki Kumar Das	__	
20.	Dipesh Patel	Nawada	01
21.	Harsh Singh	New Delhi	01
22.	Karan Kumar	Gorakhpur	01

RECOVERY MADE

- 63 Mobile Phones
- 02 Laptops
- 02 Macbooks
- 01 Tablet

PLACES WHERE RAIDS WERE CONDUCTED

S. No.	District	Place	State
1.	Jamtara	Birajpur	Jharkhand
2.		Karmatar	
3.		Narainpur	
4.		Dhumaria	
5.		Partol	
6.		Pathrol	
7.		Nauadi	
8.		Fatehpur	
9.	Deoghar	Margomunda	
10.		Sarwan	
11.		Nagadari	
12.		Sarath	
13.		Murli Pahari	
14.	Giridih	Giridih	
15.	Nawada	Kashichak	Bihar
16.	Jamui	Chakai	
17.	Asansole	Asansol	West Bengal
18.	Kolkata	Kolkata	

19.	Gorakhpur	Shakti Nagar	Uttar Pradesh

LIST OF APK FILES

Total: 32 APK files

S. No.	Name of APK File
1	HDFC KYC 8.apk
2	base.apk
3	Customer_Support_.apk
4	Desi Leaks.apk
5	appartment_booking_FUD.apk
6	Appointment booking v1.apk
7	AXIS KYC UPDATE.apk
8	Bank of India Pension Card Verification .apk
9	Gas Bill Update .apk
10	Google IPTV.apk
11	Bill Update.apk
12	RBL CARD LIMIT INCREASE.apk
13	RTO e-Challan PDF.apk
14	TATA POWER METER UPDATE.apk
15	LumaVibe.apk
16	Tu_2026_bi_8.apk
17	TATA POWER METER UPDATE1.apk
18	TATA POWER.apk
19	NextGen_mParivahan.apk
20	NightPlay.apk
21	PNB ONE 1.0 com.drx4a.servis.apk
22	PNB_ONE_HMRS_VERIFICATION_UPDATE_file.apk
23	Porn Chat.apk
24	Private 1-on-1.apk
25	PSB_Bank_Pension_Card_Apply_FUD (2).apk
26	Punjab & Sind Bank.apk
27	Meter Update (1).apk
28	PM Kisan.apk
29	PM Kisan eKYC Update.apk
30	PM Kisan Registration Form.apk
31	PM Yojana.apk
32	E-Challan.apk

MODUS OPERANDI

1. Development of the APK Generation Panel:

- Centralised APK panels developed for generating malicious Android Package Kit (APK) files were developed.

- Master User ID and password generated and Centralised access granted to Distributors.

2. Formation of a Network of Sub-Distributors:

- Access of Panel further granted to Sub Distributors with unique ID and Password on monthly rental.
- These sub-distributors operated as independent links in the network and used the panel to generate malicious APK files with different User Interface as per their requirement for targeting unsuspecting victims.

3. Generation and Distribution of Malicious APKs:

- The sub-distributors generated multiple malicious APK files through the centralised panel.
- More than 32 APK files were subsequently analysed during the investigation.
- These applications were prepared and circulated by the sub-distributors to target victims through different methods of social engineering and impersonation.

4. Identification and Targeting of Victims:

- Sub-distributors targeted potential victims by impersonating representatives of banks and other legitimate institutions.
- The victims are contacted by sending a WhatsApp message and the sender impersonates as a representative of a Bank and offered assistance in completing the Life Certificate verification process, KYC updation, credit card issuance, Paying bills of BSES and IGL connection and enhancement of credit limits etc.
- The complainant was induced to download and install an APK file on the pretext of completing the said processes
- Certain permissions such as access to the calls, messages and photo gallery etc were also obtained.

5. Compromise of Mobile Devices and Acquisition of Sensitive Information:

- Once the malicious APK files is installed, the accused persons gain unauthorised access to information and functionalities of the victims' mobile devices
- With permissions granted the accused persons were able to obtain sensitive personal and banking-related information, which were exploited for carrying out fraudulent transactions.

6. Exploitation of Banking Information and Fraudulent Transactions:

- The victims' banking details were used to carry out unauthorised financial transactions.
- The cheated amount is used to place orders from instant delivery applications such as Flipkart Minutes, Swiggy Instamart, Bigbasket etc and purchase mobile phones, Silver coins and Gift coupons.

7. Post-Operation Action, Transit & Investigation

Legal formalities, safe transportation and further investigation.

- Completion of necessary arrest and seizure formalities at the respective locations.
- Timely production of arrested accused persons before the competent courts and completion of transit-related legal formalities.
- Coordinated transportation of the arrested accused persons and seized case property to Delhi.
- Preservation and examination of the recovered digital evidence.
- **Assessment of the impact of the operation through NCRP complaint data, including the decline in reported APK-fraud complaints from 1,406 to 724 in the comparison periods.**

Accused persons were arrested one two cases among other same MO cases, vide e-FIR No. 0567/2026, u/s 318(4)/319(2)/112(2)/61(2)/3(5) BNS PS cyber West & was registered at PS Cyber West and e-FIR 0522/26 U/S 318(4)/319(2)/61(2)/3(5) BNS PS cyberWest.

(HARESHWAR V. SWAMI, IPS)
DY. COMMISSIONER OF POLICE
WEST DISTRICT, DELHI