Cybercrime Incidents in France and India Expose Global Fraud Models

Infosources™

August 24, 2025

From Paris to Mumbai, two very different cybercrime cases reveal the same reality: digital fraud has become both a high-tech service industry and a grassroots exploitation machine. In France, an Android banking trojan sold like a subscription app is siphoning money from users of major banks. In India, slum residents' identities were turned into pipelines for global fraud networks moving tens of crores of rupees. Together, these incidents show how cybercrime now thrives at both ends of the spectrum—leveraging cutting-edge malware and low-cost human vulnerabilities to fuel an interconnected underground economy.

Two separate incidents—one centered on Android malware in Europe and another involving large-scale identity fraud in India—illustrate how cybercrime continues to evolve, combining sophisticated digital tools with systemic exploitation of vulnerable populations.

In France, the spotlight is on *DroidBot*, the latest in a series of highly adaptive Android banking trojans. What sets DroidBot apart is both its professionalized "malware-as-a-service" business model and the scale of its targeting. First active in mid-2024 and only detected later in the year, DroidBot was built by Turkish cybercriminals and is sold for about $3,000 a month. At least 17 different groups are already deploying it.

The malware masquerades as legitimate apps—including Chrome, the Play Store, or even a fake "Android Security" application. Once installed, it takes control of the victim's device. Its functions include recording keystrokes, intercepting SMS (including banking OTPs), overlaying fake banking screens, and enabling full remote access. These capabilities exploit Android's accessibility services, a recurring weak point in mobile security.

The impact in France is substantial. Eight major banks—Boursorama, BNP Paribas, Crédit Agricole, Axa Banque, Caisse d'Épargne, Banque Populaire, ING, and Société Générale—are specifically targeted, though dozens of other institutions worldwide are also in the crosshairs. Attacks are not limited to France: victims in the UK, Italy, Germany, Spain, Portugal, and Turkey have also been reported. French authorities emphasize that this is not a breach of the banks themselves but rather of individual users who inadvertently install the malware.

Researchers confirm that DroidBot is actively maintained. Its authors provide updates, run Telegram-based "customer support," and continuously localize the malware for different markets and languages. Analysts warn that the model is scalable and could soon expand to Latin America, where mobile banking fraud is already widespread. For financial institutions, the case is a reminder that their security perimeter extends beyond internal systems to the personal devices of customers. For users, it demonstrates how trust in familiar app logos and app stores can be manipulated into opening the door to theft.

Meanwhile, in India, Mumbai Police uncovered a sprawling ₹60 crore cyber fraud network operating out of Kandivali East. Investigators found two front companies—DJ Search Consultancy and Pririt Logistics Private Limited—were being used to provide "money mule"

accounts to overseas syndicates. Five individuals were arrested, and a large cache of evidence was seized, including laptops, mobile phones, SIM cards, debit cards, cheque books, and hundreds of bank documents.

The method was simple but effective. Recruiters targeted slum residents, paying them small sums in exchange for their identity documents. With these papers, the group opened nearly a thousand bank accounts, none of which were actually controlled by the nominal owners. Instead, the accused managed these accounts and rented them out to foreign fraud operators in Cambodia, Thailand, China, and Malaysia. These accounts became pipelines for illicit flows linked to digital arrest scams, online shopping fraud, and fake trading platforms.

Investigators have already traced at least 339 of these accounts flagged in the national cybercrime system. Police estimate the total turnover of the operation at about ₹60 crore, with notable diversions traced to Mumbai itself (₹1.67 crore) and to wider Maharashtra (₹10 crore). Evidence suggests that the accounts were integrated into a broader laundering infrastructure that enabled international crime groups to rapidly circulate and disguise stolen funds.
The case demonstrates how easily vulnerable populations can be exploited, often without understanding the implications of handing over their identity documents. It also highlights the critical role of local facilitators in building the infrastructure that transnational fraud groups depend on. For Indian law enforcement, the challenge lies in detecting and blocking mule networks before they scale further; for the financial system, the pressure remains on identity verification and account monitoring as persistent weak points.

Taken together, the French and Indian cases illustrate complementary aspects of the cybercrime ecosystem. DroidBot shows how malicious tools are commercialized as subscription-based products, while the Mumbai fraud reveals how physical-world vulnerabilities—such as poverty and lack of digital literacy—are weaponized to enable global scams. Both cases expose systemic weaknesses, whether in mobile platforms or in identity verification, that continue to provide entry points for financial crime worldwide.