

Forum:[Hack Forums](#)

Thread: [Android malware uses dropper apps to steal SMS and OTPs](#)

JoseMar - December 22, 2025, 1:30 am

Android malware uses dropper apps
to steal SMS and OTPs

Been reading up on some recent Android malware stuff and yeah... this is getting ugly.

Attackers aren't sending "obvious" trojan APKs anymore.
Now it's dropper apps pretending to be legit, Google Play, videos, photos, even wedding invitations.
Looks harmless. Isn't.

Once installed, it drops Wonderland (ex-WretchedCat).
Basic idea? SMS stealer, but on steroids.

It grabs SMS + OTPs, runs USSD commands, hides notifications, and talks back to C2 in real time.
Basically turns your phone into a remotely controlled ATM drain.

Main target so far: Uzbekistan.
Distribution is classic social engineering but scaled:
fake Google Play pages, Facebook ads, dating apps, and Telegram spam using already hijacked accounts. One infected user = more victims. Loop continues.

What stands out to me is how organized this is.

APK builds generated via Telegram bots, rotating C2 domains, workers getting a cut, separate roles for devs, owners, card checkers. This isn't some kid with an APK binder.

And it's not just Wonderland either: Cellik RAT literally has a one-click builder that wraps malware into legit Play Store apps.

Frogblight pushes fake court docs via SMS.

NexusRoute abuses fake government portals and GitHub-hosted APKs.

Feels like Android malware has crossed a line.
More obfuscation, more automation, less skill needed, bigger scale.

Not "spray and pray" anymore.
This is mobile fraud as a service.

And yeah... it's only going to get worse.