New Android malware lets criminals use your bank card in real time

by Pieter Arntz | August 13, 2026

Researchers at Group-IB have discovered a new NFC relay malware family, purpose-built to capture live card data via NFC and forward it in real time to attackers. They dubbed it "WindRelay."

NFC (Near Field Communication) is wireless technology that allows devices such as smartphones, payment cards, and payment terminals to communicate when they're very close together. So, instead of stealing your physical bank card, the attackers capture NFC activity on an infected mobile phone and relay it in real time to a criminal-controlled device held against a contactless payment terminal, or an ATM that supports contactless cash withdrawals.

The researchers describe a 13-minute call impersonating a bank, in which a victim was persuaded to install an Android app labelled with the bank's name. That app was a remote access Trojan (RAT) called **SpyNote**. SpyNote gave the attacker remote control of the phone and enabled the quiet installation of a second app, **WindRelay**.

The attackers then opened the victim's legitimate banking app remotely and arranged a loan in the victim's name, while also asking them to tap their physical payment card against the phone and enter its PIN. That tap let the second app forward the card's contactless data in real time to the criminals, allowing them to make purchases or, in some cases, withdraw cash from an ATM.

This division of tasks is the important development here. The remote-access malware (SpyNote) gets the attackers into the phone, and the NFC relay malware (WindRelay) turns the victim's physical card into something the criminals can use elsewhere at that moment.

It's not quite as simple as it sounds, because NFC comes in a few different "flavors." Some produce a static code. Take the card that opens my apartment building door, for example. That kind of signal can easily be copied to a device like my Flipper Zero so I can use it to open the door. But sophisticated contactless payment cards use dynamic codes. Each time you tap to pay, your card's chip generates a unique, one-time code (often called a cryptogram or token) that cannot be reused.

That's why the critical feature of NFC relay malware is real-time relaying. Since payment card transactions use dynamic, transaction-specific cryptographic data, timing is central to this kind of fraud.

The telephone call isn't just the lure. It's also the attackers' control channel. It lets them overcome the victim's hesitation, respond to confusion instantly, and coordinate the precise moments when the victim installs an app, taps their card, and enters a PIN.

This is part of an established and expanding NFC relay fraud category sometimes called **ghost tapping**. In the past, we've discussed NGate and SuperCard X, which are similar malware families. But the combination with SpyNote is what makes this campaign stand out.

How to protect yourself

As with many security threats, the best defense is you. The cybercriminals behind this attack can't do anything unless you install the software on your phone, so they go through several steps to convince you to do so.

- Be sceptical of calls and text messages from people you don’t know, especially those claiming to be urgent. Scammers typically try to panic you into acting quickly. Once they get you on the phone, they can build trust, making it harder to think critically and say no.
- If you feel compelled to take action, check in with someone you trust first. If you’re still convinced the request is genuine, verify the message independently. Call your financial institution using an official number, not through the one in the text message or email.
- Never give personal details to anyone who contacts you unexpectedly, and never change your banking details at their request. A bank will not ask you to install an app from a link, text message, browser download, or other unofficial source to “secure” your card.
- Avoid sideloading apps (installing them from outside of the Google Play store), and treat unexpected Accessibility or device-control permissions as a serious warning sign.
- Use an up-to-date, real-time anti-malware solution to protect your devices.