

Gone with the WindRelay: A New Malware Combo Behind a Growing Fraud Scheme

 group-ib.com/blog/windrelay-nfc-spynote-rat-combo-fraud

Yauheniya Mazurenka

August 12, 2026

Malware Profile





SpyNote

Platforms
Android

First seen
2016

SpyNote is a malware family of Android Remote Administration Tools (RAT) that enables a threat actor to control victims' devices. SpyNote was leaked on underground forums in mid-2016 as cracked versions for free downloading. SpyNote RAT has the ability to monitor SMS (text) messages, access the microphone, record audio, access the camera, contacts, calls, files, GPS data, load applications, utilize proxies, persist after a reboot, and open a shell to the phone. SpyNote malware family has evolved over time, with the adoption of cutting-edge methods and technologies.

Used by

Various

Techniques

- T1398 - Persistence -> Boot or Logon Initialization Scripts
- T1626.001 - Privilege Escalation -> Abuse Elevation Control Mechanism -> Device Administrator Permissions
- T1417 - Credential Access -> Input Capture
- T1426 - Discovery -> System Information Discovery
- T1512 - Collection -> Video Capture
- T1513 - Collection -> Screen Capture
- T1481.002 - Command and Control -> Web Service -> Bidirectional Communication
- T1646 - Exfiltration -> Exfiltration Over C2 Channel

Group-IB, 2026

Introduction

Contactless payment fraud has moved from a theoretical risk to an operational one, and the scale is now visible in both industry and regulatory reporting. The European Payments Council's [2025 Payment Threats and Fraud Trends report](#) identifies NFC relay fraud — and the related “Ghost Tap” technique — as a rising category, noting it frequently overlaps with remote access scams and results in unauthorized transactions and a complete loss of control over funds, with victims sometimes unknowingly drawn into money laundering as a result. The scale behind that assessment shows up clearly in independent telemetry: NFC-based attacks

on Android devices rose 188% in the first four months of 2026 compared to the same period in 2025, with 35,600 attacks blocked in that window alone, up from over 12,300 a year earlier ([Kaspersky](#)); this followed a more than 35-fold increase in NFC-related attacks recorded in the first half of 2025 compared to the second half of 2024 ([ESET](#)).

Law enforcement attention has followed the same trajectory, and Central and Eastern Europe has been at the center of it. The first documented attacks using a modified version of the open-source NFCGate tool occurred in late 2023 in the Czech Republic ([Kaspersky](#)), and in March 2024, Czech Police confirmed the arrest of a 22-year-old individual after receiving reports of a suspicious individual withdrawing money from ATMs in Prague without using any physical card. Despite that arrest putting the group's activity on hold at the time, the same NGate tooling was later observed spreading to other regions ([ESET](#)). That spread has continued: Zimperium researchers have tracked NFC relay campaigns broadening across Poland, the Czech Republic, and Slovakia, supported by more than 70 identified command-and-control servers and distribution hubs ([Zimperium](#)), and threat actors have gone as far as impersonating the National Bank of Slovakia directly, to lend credibility to malicious apps and obtain the NFC permissions needed to carry out the fraud ([GBHackers](#)).

Group-IB have tracked this category closely ourselves. In our own research, [Ghost Tapped: Tracking the Rise of Chinese Tap-to-pay Android Malware](#), we documented Chinese-language Fraud-as-a-Service operations distributing NFC-enabled Android malware across Telegram, with more than 54 malicious samples identified and at least \$355,000 in confirmed fraudulent transactions linked to a single point-of-sale vendor between November 2024 and August 2025 alone.

This report sits alongside that body of work, but its focus is different: rather than analyzing a single incident, we look at a technique — a new, purpose-built NFC relay [malware](#) family, tracked here as WindRelay, deployed together with a known [RAT](#), SpyNote, inside a live-call [social-engineering](#) scheme. The case study that follows illustrates this combination in practice, but the pattern itself is what matters: RAT-driven remote access opens the device up, and NFC relay malware turns a single card tap into a cash-out channel.

Key discoveries

- **A previously unseen NFC relay malware family**, purpose-built to capture live card data via NFC and relay it out in real time.
- **This NFC malware is deployed together with SpyNote, a known RAT.** SpyNote's Accessibility Service access lets the fraudster sideload and activate the NFC app silently, with no screen sharing ever triggered.

- **This NFC + RAT pairing is a significant finding** that shows the new NFC tooling is not used standalone, but as part of a combined toolkit with established remote-access malware.
- **The RAT's app label used the victim's own name.** This is a deliberate trust-abuse tactic that acts as unspoken proof that the caller already knows the victim, lowering suspicion and personal defenses.
- **The NFC malware's permission set reveals deliberate, engineered design:** NFC for capture, INTERNET for real-time exfiltration, READ_CONTACTS for further targeting, an unusual DUMP permission for device inspection, and custom self-defined permissions to resist security tooling.
- **Dual monetization within a single scheme:** RAT-driven remote access can be used to take out a digital loan, while the NFC malware enables physical, card-present purchases..

Who may find this blog interesting:

- Cybersecurity analysts and corporate security teams
- Malware analysts
- Threat intelligence specialists
- Cyber investigators
- Computer Emergency Response Teams (CERT)
- Law enforcement investigators
- Cyber police forces

Group-IB Threat Intelligence and Fraud Protection Portals:

Group-IB customers can access our Threat Intelligence and/or Fraud Protection portals for more information about the malware and scheme described in this blog.

Threat Intelligence:

- [SpyNote](#)
- [WindRelay](#)

Fraud Protection:

- [NFC Relay + RAT Banking Fraud Scheme \(SpyNote + WindRelay\)](#)
- [SpyNote](#)



SpyNote

Platforms
Android

First seen
2016

SpyNote is a malware family of Android Remote Administration Tools (RAT) that enables a threat actor to control victims' devices. SpyNote was leaked on underground forums in mid-2016 as cracked versions for free downloading. SpyNote RAT has the ability to monitor SMS (text) messages, access the microphone, record audio, access the camera, contacts, calls, files, GPS data, load applications, utilize proxies, persist after a reboot, and open a shell to the phone. SpyNote malware family has evolved over time, with the adoption of cutting-edge methods and technologies.

Used by

Various

Techniques

T1398 - Persistence -> Boot or Logon Initialization Scripts

T1626.001 - Privilege Escalation -> Abuse Elevation Control Mechanism
-> Device Administrator Permissions

T1417 - Credential Access -> Input Capture

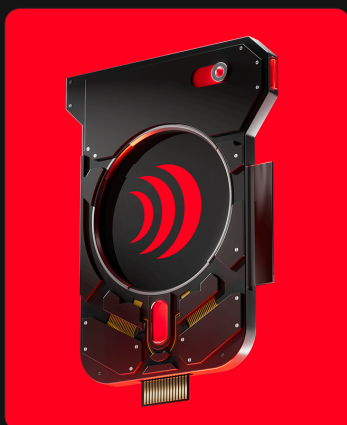
T1426 - Discovery -> System Information Discovery

T1512 - Collection -> Video Capture T1513 - Collection -> Screen Capture

T1481.002 - Command and Control -> Web Service -> Bidirectional Communication

T1646 - Exfiltration -> Exfiltration Over C2 Channel





WindRelay

Platforms
Android

First seen
22 August 2025

WindRelay is a custom-built Android NFC relay malware designed to conduct real-time contactless payment card relay attacks. The malware consists of two companion components that operate in tandem: a reader component installed on the victim's device, which interfaces with the victim's physical payment card via NFC, and an emulator component installed on the threat actor's device, which emulates the card at a payment terminal. The two components communicate through a shared command-and-control infrastructure over WebSocket, relaying EMV APDU commands and responses between the terminal and the victim's card in real time.

Techniques

T1660 - Initial Access -> Phishing

T1398 - Persistence -> Boot or Logon Initialization Scripts

T1417.001 - Credential Access -> Input Capture -> Keylogging

T1426 - Discovery -> System Information Discovery

T1636.003 - Collection -> Protected User Data -> Contact List

T1481.002 - Command and Control -> Web Service -> Bidirectional Communication

T1646 - Exfiltration -> Exfiltration Over C2 Channel



Group-IB, 2026

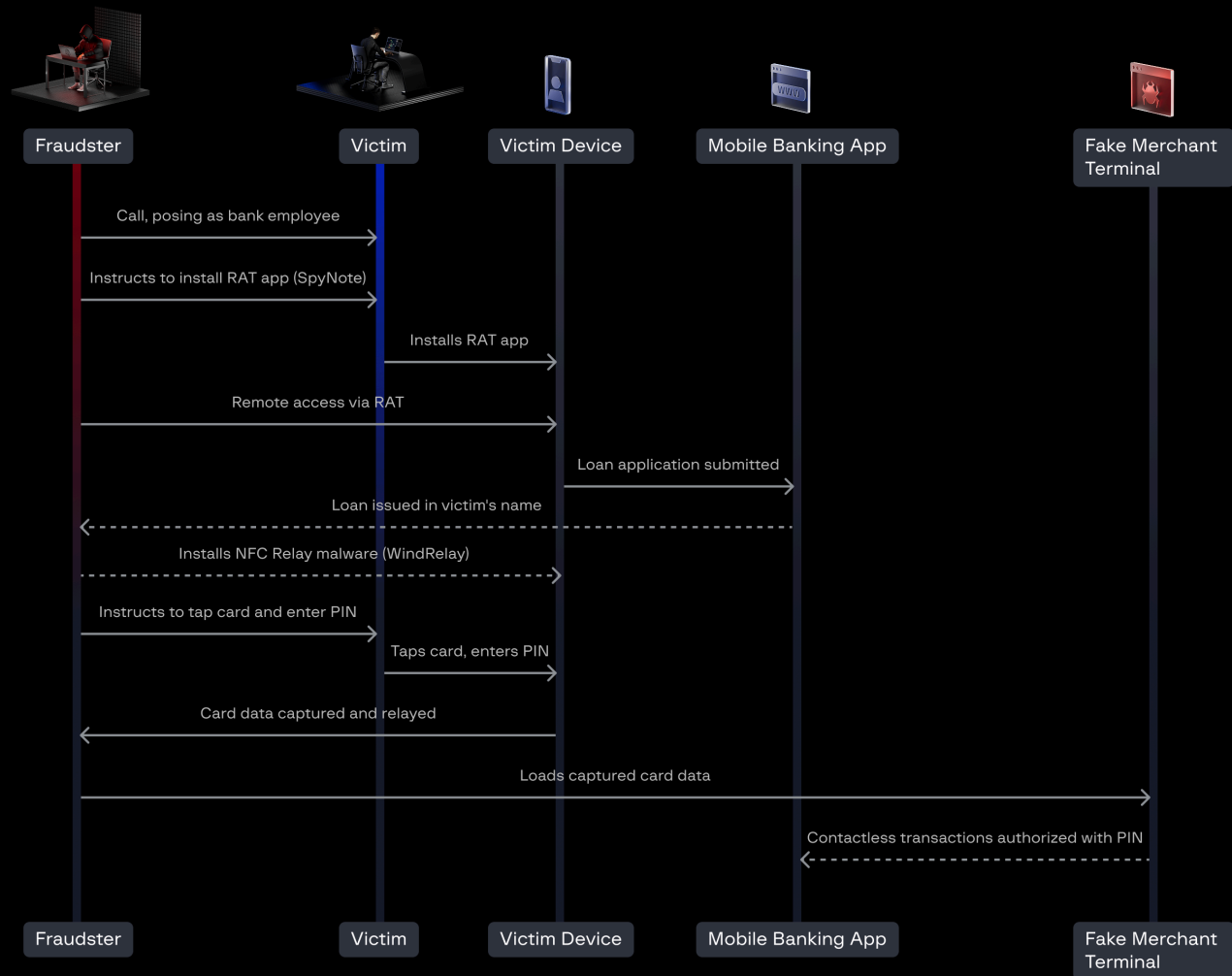
Description and Case Overview

The following case study, derived from an investigation supported by Group-IB's Fraud Protection team for a client, provides a detailed illustration of how this purpose-built NFC malware, tracked as WindRelay, and the SpyNote RAT are deployed in tandem.

In one 13-minute phone call, the victim installed a RAT onto their own device — everything after that was performed by the fraudster. By the end of the call, the fraudster had taken out a loan in the victim's name through remote access to the victim's mobile app, and was streaming their card data to a fake merchant terminal. Every transaction was approved using the PIN the victim had entered themselves. The victim stayed on a live call with the fraudster for the entire incident.

WindRelay NFC + SpyNote RAT Banking Fraud Scheme

Attack Chain Overview



Group-IB, 2026

Figure 1: Attack chain overview.

Key actions during the call, in order:

1. The fraudster called the victim posing as a bank employee, claiming a problem with their bank card.
2. The victim installed the first app — a RAT, labeled with the victim's own name — after being guided to do so by the fraudster on the call.
3. Using the RAT's remote access features, the fraudster then installed a second app — the NFC relay malware — without needing any additional input or action from the victim.
4. Once remote access was in place, the fraudster also took the opportunity to issue a loan in the victim's name. Our investigation indicates that this was likely an add-on to maximize the payout, not a separately planned step.
5. The victim tapped their card to their phone and entered their PIN, as instructed.

Shortly after the call ended, physical card transactions started appearing on the victim's account, which the bank confirmed were linked to NFC relay activity.

What exactly happened? Breaking down the scam

Utilizing a phone call as a control channel

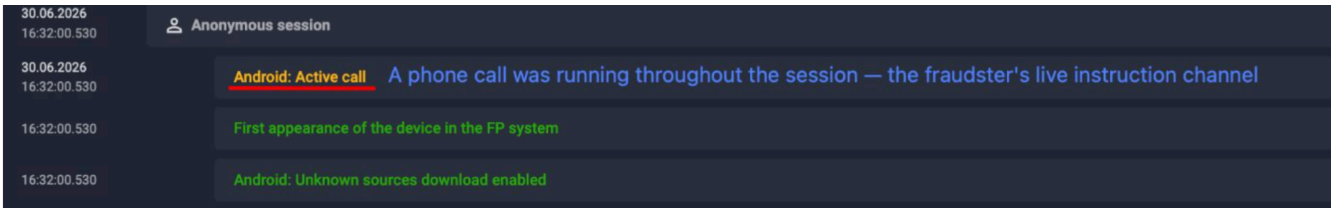


Figure 2: Active call early detection (before the authorization).

Group-IB Fraud Protection detected an active call running for the whole session. This is an important factor in this scheme: the fraudster did not rely on one-time instructions, like a phishing link or SMS code. Instead, they kept live, real-time control over the victim throughout the attack. Every step that followed — installing apps, approving the loan — happened while the victim was being guided live on the call.

Sideloaded a personalized RAT mid-call

During the same call, the [Group-IB Fraud Protection](#) detected a remote access trojan (RAT) installed through the device's package installer — the standard way to sideload apps outside an official app store. This sample's app label was personalized with the victim's own name, not a generic or impersonated brand. This is possible because SpyNote is distributed with a builder toolkit that lets an operator compile each APK with a custom app name, label, and package name before deployment — personalization isn't a manual, one-off effort, it's a built-in option in the tooling.



Figure 3: Detected sideloaded RAT.

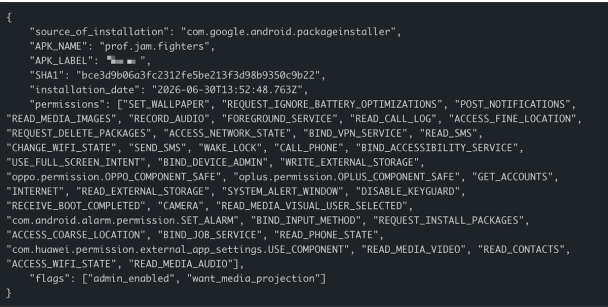


Figure 3: Detected sideloaded RAT.

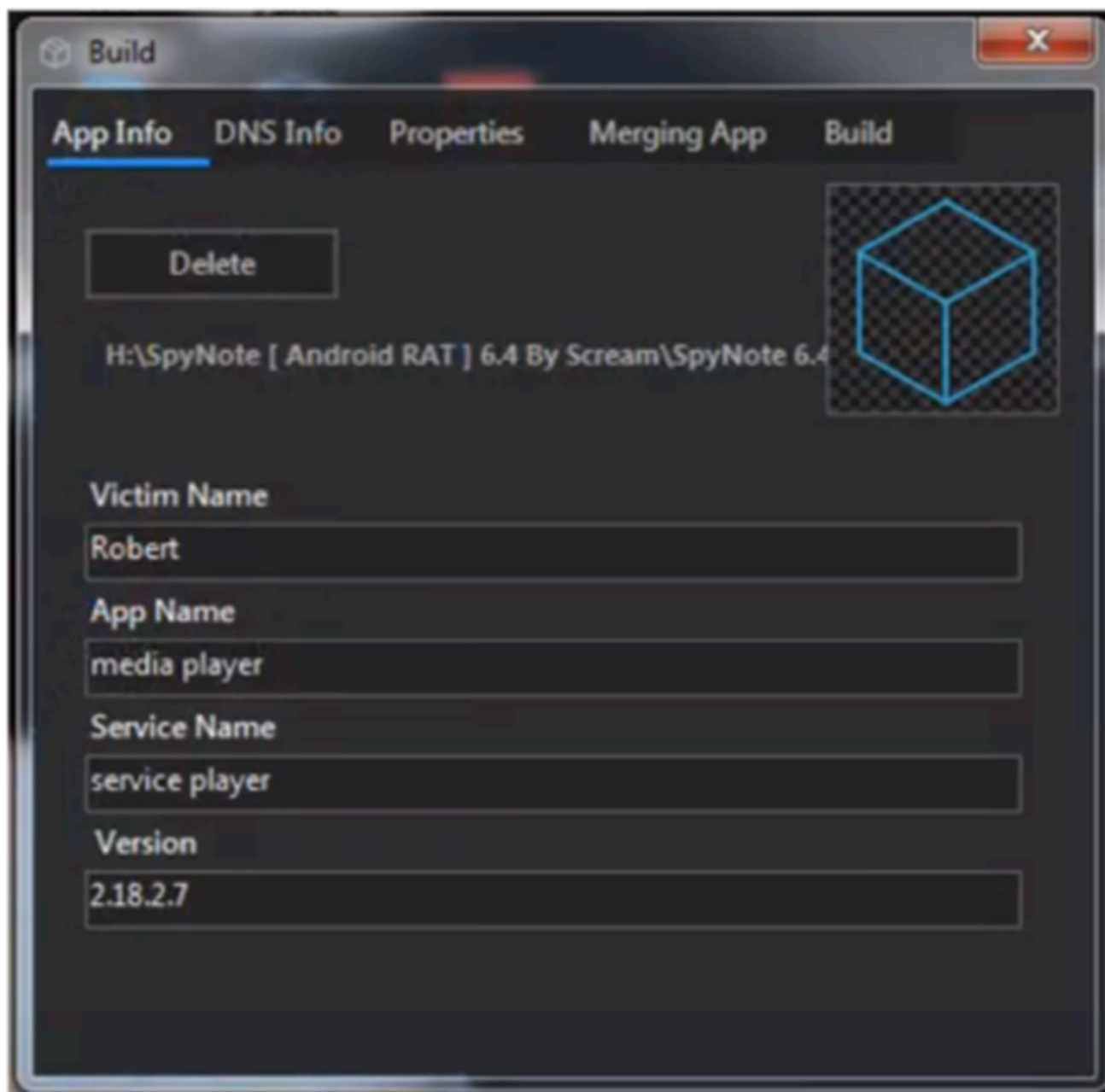


Figure 4: SpyNote APK Builder allows for data customization.

The use of target-specific labels is a critical finding: it indicates a delivery process tailored to the individual rather than a generic, mass-distributed payload. This implies a degree of pre-call reconnaissance where the threat actor harvested basic PII — specifically the victim's name and phone number — to ground the social-engineering pretext and compile a personalized APK. Such tactics are more effective at weakening a victim's natural defenses and suspicions. It removes the one cue people are trained to check before installing something unfamiliar — a strange or generic app name — right at the moment they're most likely to hesitate.

NFC relay malware installation

Group-IB Fraud Protection detected a second application — built to relay NFC card data — installed via the package installer while the RAT's remote access was already active. The fraudster used that access to push the install himself, rather than the victim downloading or approving it directly, from a source with no legitimate standing on the device. This second install happened shortly after the RAT install, while the call was still ongoing.

The screenshot displays a security analysis interface with two main panels. The left panel shows a list of events for a session with ID 74963485-7490-11f1-b14a-a2e1c08493ad. The events include 'Android: Active call', 'First appearance of the device in the FP system', 'Android: Unknown sources download enabled', 'Protected application installed recently', 'Android: Accessibility service', 'Protected application installed N days ago', and 'Installed NFC application after active call' (highlighted with a red arrow). The right panel shows the 'Installed NFC application after active call' details, including the score (80), category (Android), and a list of permissions: 'ACCESS_NETWORK_STATE', 'app.blaze.monitor.permission.VSLTPMYT', and 'app.blaze.monitor.permission.VSLTPMYT'.

Session: 74963485-7490-11f1-b14a-a2e1c08493ad

Filters: Event

Session ID: 74963485-7490-11f1-b14a-a2e1c08493ad Device ID: 03d342f9-8d14-4657

Anonymous session

Android: Active call

First appearance of the device in the FP system

Android: Unknown sources download enabled

Protected application installed recently

Android: Accessibility service

Protected application installed N days ago

Installed NFC application after active call

Android: Application downloaded from a non-legitimate source

Android: Application from a non-legitimate source has access to read sms.

Android: Application downloaded from a non-legitimate source

Android: Application from a non-legitimate source has access to NFC

Android: Application from a non-legitimate source has access to read sms.

Android: Application downloaded from a non-legitimate source

Android: Application from a non-legitimate source has access to admin privileges.

Android: Detected fake application has access to admin privileges

Installed NFC application after active call

30.06.2026 at 16:32:59

Threat details

Score	Category	Status
80		Android

Data

```
{
  "call_was_in_sessions": ["74963485-7490-11f1-b14a-a2e1c08493ad"],
  "source_of_installation": "com.google.android.packageinstaller",
  "APK_NAME": "app.blaze.monitor",
  "APK_LABEL": "Dropstab brana",
  "SHA1": "8f389b7d18c0ea9582a03f11d1b5320c885cf517",
  "installation_date": "2026-06-30T14:12:02.310Z",
  "permissions": ["ACCESS_NETWORK_STATE", "app.blaze.monitor.permission.VSLTPMYT", "app.blaze.monitor.permission.VSLTPMYT"]
}
```

Description

An app from a non-legitimate source with access to the NFC module was installed within 24 hours of an active call

Figure 5: NFC malware sample detection.

Analyzing the requested permissions, Group-IB researchers were able to map directly what the attacker could now do with the NFC malware:

- **NFC** — The core capability. Once granted, the app could read card data the moment the victim taps it to their phone, capturing what was needed to use the card at a fake terminal.
- **INTERNET / ACCESS_NETWORK_STATE** — Gave the attacker a live channel to send this data out in real-time, so the card could be used within moments of the tap.
- **READ_CONTACTS** — Let the attacker reach beyond the immediate victim, possibly to find new targets or support further social engineering.
- **DUMP** — An unusual permission for a third-party app. It suggests the attacker could inspect deeper device or system state, possibly to check for security tools or confirm the compromise was working.
- **Custom <apk_name>.* permissions** — Used to isolate the app's internal components from other apps on the device, making it harder for security software to interfere or inspect the malware.

Together, these permissions gave the fraudster everything needed to turn one moment — the card tap — into a live, remotely usable card clone, without ever seeing the victim's screen or needing an official app store listing.

Performing the fraud live: Card funds cash-out

With the NFC relay app active and remote access already in place, the fraudster — still on the same phone call — told the victim to tap their bank card against their phone. That tap was the moment of capture: the app read the card data via NFC and sent it out through the attacker's remote session.

What's stolen: Not a static card number, but the live data exchange between the card's chip and a reader at the moment of the tap — including the one-time authentication code the card generates for that specific transaction.

How it's stolen: The relay malware turns the victim's phone into a fake contactless reader (like a POS). When the card is tapped to the phone, the malware communicates with the card's chip over NFC exactly as a real POS-terminal would, capturing that live exchange instead of a terminal doing so.

How it's transmitted: The captured exchange is streamed out over the internet, in real time, to a second device in the fraudster's hands — not stored and reused later, but relayed as it happens. This is exactly why INTERNET permission is set on the NFC malware.

How NFC relay is used to fraudulently pay for items or withdraw funds: That second device controlled by the fraudster, presents itself as the card to a real merchant terminal or ATM, at the same moment the victim's card is being read. In effect, the victim's card and the real terminal are still talking directly to each other — the fraudster's setup is just an invisible relay in between, passing the exchange back and forth across a distance. Because the terminal is genuinely completing a live handshake with a real card, the transaction goes through and processes the withdrawal or purchase as normal.

Malware Attribution

The NFC relay application is an independently developed Android malware that draws on NFC relay techniques. Using metadata of detected malicious applications, Group-IB's Fraud Protection team correlated them to other applications used in multiple campaigns targeting victims in Czechia, Slovakia, and Slovenia. We identified 23 samples uploaded to VirusTotal between November 2025 and July 2026. The samples mimic various institutions from the targeted countries and contain text in the language of each targeted country. Some samples contain personalized UI elements and labels, such as the name of the victim, similar to the

personalized RAT. This suggests the threat actor behind these campaigns most likely has the capability to dynamically build malicious applications tailored to individual victims. Group-IB Threat Intelligence tracks this malware as [WindRelay](#). Our researchers also identified 4 Command and Control (C2) IPs used by this malware to relay NFC data. The C2 IPs and the identified VirusTotal samples are in the *Indicators of Compromise* section below.

The RAT's personalization pattern and its metadata has allowed our team to attribute it to a [variant of SpyNote](#).

VirusTotal samples connected to this case carry confirmed fraudulent attribution, corroborating both the malware family identification and the fraudulent intent behind the deployment.

Conclusion

This case shows that modern fraud rarely relies on one technique. Here, the fraudster combined three capabilities in a single session — a live social engineering call, a personalized RAT for remote device control, and an NFC relay malware for physical cash-out. The fraudster also used these capabilities to hit two separate payout channels — a digital loan and card-present purchases — before the bank or victim could react.

Beyond the details of this single case study, the tooling of the malware package in this scam scheme also presents several important indicators of an evolving fraud ecosystem:

- **No screen sharing does not mean no remote access.** This case shows a RAT achieving full remote control without ever triggering screen-share detection.
- **The RAT's label was personalized with the victim's name.** This points to a delivery process tailored per target, not one generic payload sent to everyone. This detail is itself useful for detection.
- **Tight Timing.** The NFC app was installed from a non-legitimate source shortly in a matter of minutes after the call began and the malicious RAT install.
- **The fraudster used two payout channels in one session.** This shows attackers diversifying how they cash out within a single victim engagement, rather than relying on a single, fixed method or script.
- **This NFC relay tool is not a one-off.** Using a permission- and certificate-based hunting approach, Group-IB researchers found other confirmed-fraudulent samples using the same tooling. This means the detection signature described here applies beyond this single incident.

Recommendations

Detection

- Leverage advanced [Threat Intelligence](#) services for the latest information and updated threat feeds.
- Implementing a robust [Fraud Protection](#) session monitoring system will enable the detection of malicious applications on user devices, as well as unusual behavior and logins from compromised devices.
- Don't rely on screen-sharing detection alone as a proxy for remote access. Add checks for RAT indicators that don't require screen sharing — Accessibility Service abuse, sideloaded apps installed mid-call, or apps granted admin/device-admin privileges shortly after a call starts.
- Alert installations of apps from non-official sources (package installer, not Play Store) that occur during an active call. This timing pattern is a strong signal on its own, independent of what the app does.
- Build detection around app permission sets, not just known malware hashes. This can help catch new samples before they're individually identified.

Prevention

- Treat “personalized” app labels (using the victim's own name) as a specific red flag in fraud awareness materials — this detail is unusual enough to be memorable and actionable for customers.
- Apply extra friction (step-up authentication, cooling-off periods, out-of-band confirmation) to loan applications submitted while other risk signals are present, such as an active call or a recently installed unfamiliar app.
- Consider velocity or correlation rules that flag when a loan disbursement and a physical card transaction occur close together for the same customer — this combination is unusual for genuine activity and matches the dual-monetization pattern seen here.

Response

- When a customer reports a fraud call, ask specifically whether they installed any apps during the call and, if possible, retrieve the app names/labels/files — this is often lost if not captured early, as it was here.
- Treat confirmed NFC relay cases as a signal to check the customer's account for other channels that could have been touched in the same session (loans, transfers, new payees), not just the transaction type initially reported.

Acknowledgement of research support:

[Pavel Naumov](#), Senior Security Researcher • Global Fraud Protection BU

Frequently Asked Questions (FAQ)

1. What's the difference between WindRelay and SpyNote, the two malware identified in this scam scheme?

arrow_drop_down

SpyNote is a [Remote Access Trojan \(RAT\)](#) that grants fraudsters remote control over a victim's device, enabling them to navigate mobile banking applications and silently install additional apps. WindRelay, on the other hand, is a custom NFC relay malware specifically designed to capture contactless payment card data in real-time when a card is tapped against the phone and relay it to an attacker's terminal.

2. How do fraudsters gain access to the victim's device?

arrow_drop_down

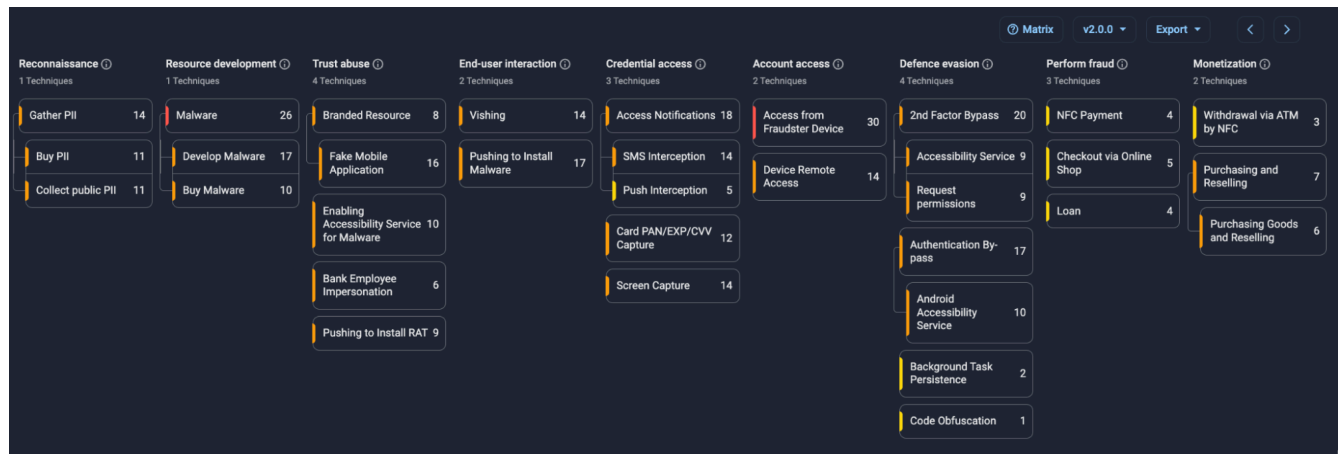
Fraudsters gain initial access through a [social engineering](#) call posing as a bank employee to report a "problem" with the victim's bank card. This pretext allows the fraudster to guide victims into manually installing a personalized SpyNote RAT application. Once SpyNote is installed, the fraudster leverages its remote access permissions to silently sideload the WindRelay malware onto the device without requiring any further victim action.

3. How are victims affected by this scheme?

arrow_drop_down

Victims suffer direct financial losses through a dual-monetization scheme, where fraudsters take out digital loans in the victim's name and execute unauthorized card purchases or ATM cash-outs using relayed NFC card data.

Group-IB Fraud Matrix



Indicators of Compromise (IOCs)

WindRelay NFC Malware IOCs

IOC	Type
88[.]86[.]124[.]114	C2 IP
185[.]100[.]87[.]116	C2 IP
185[.]100[.]87[.]223	C2 IP
213[.]218[.]160[.]48	C2 IP
852322e063872a025b711d5adf08531eac36a265	SHA1
11f9fb29f2cc142e81c804f53599ae36282c95b3	SHA1
50cf07b97ef999e9fc5c7efae19d0e5f39db39fa	SHA1
850680506df7892d43b3382f0f89a06ef18837c7	SHA1
1371b2b2da10ed178d26a7aad191634553f865ae	SHA1
91e66d640b2a570bd83b408b51ebbf21e95e7469	SHA1
39060c673aefa0902cb5fc787fa53364cad9ed6f	SHA1
e2e836d16a1b50d4d091f7ae507b82c0a8e05376	SHA1

56b819cb285dbdbc307268b4fadbddaa61319bb8	SHA1
a1574476a616599a202cc731a6d5dbf9b3a635f0	SHA1
48d011117eacf57128c7e473bb5d4d69e3d41ef6	SHA1
ec730da64f9feae4259ebc88113c5cebdf2b1ad7	SHA1
8e665c12b7d8e80c72d86ed4425663ecd74e453c	SHA1
67e2a1e8ab963086bb768b28307cf58dadb0acc7	SHA1
294ecf0550308dff9df0eea86ca127c064b3bfb8	SHA1
65ca7e9363539282c2670dfab100b75c9bfb6253	SHA1
dfd19ee8b550f21b99d63ce87d039d1e8e1e111b	SHA1
217ab41d543278d0ecce797a71ef38a6bc1493fe	SHA1
82a35dd0ec20791bc3161a87fdb6caa68fd3d4a6	SHA1
6feeba25748996d3928f11ef774122e02b4b8850	SHA1
1eac0c636edf181eec0315ffe3b5b1e310b1a352	SHA1
ea2be784b2c08cd6f116e14079d6583ba606c556	SHA1

SpyNote RAT Malware IOCs

IOC	Type
e05575afe5a01d150daa8b4bb935213cc0e538f6	SHA1
193078cda795dc2f12983e9b66821f7e67c6495d	SHA1
38ca1bc31ccdc1c650720abd76bcc619532c0166	SHA1
22fa5c967b0775c3f3398dcf5dbb46ff80e1708b	SHA1
bce3d9b06a3fc2312fe5be213f3d98b9350c9b22	SHA1
bc2bce53d71533c2eb1ccc30ef252ea2774d0100	SHA1

DISCLAIMER: All technical information, including malware analysis, indicators of compromise and infrastructure details provided in this publication, is shared solely for defensive cybersecurity and research purposes. Group-IB does not endorse or permit any unauthorized or offensive use of the information contained herein. The data and conclusions represent Group-IB's analytical assessment based on available evidence and are intended to help organizations detect, prevent, and respond to cyber threats.

Group-IB expressly disclaims liability for any misuse of the information provided. Organizations and readers are encouraged to apply this intelligence responsibly and in compliance with all applicable laws and regulations.

This blog may reference legitimate third-party services such as Telegram and others, solely to illustrate cases where threat actors have abused or misused these platforms.

This material is provided for informational purposes, prepared by Group-IB as part of its own analytical investigation, and reflects recently identified threat activity.

All trademarks referenced herein are the property of their respective owners and are used solely for informational purposes, without any implication of affiliation or sponsorship.

© 2003 – 2026 Group-IB is a global leader in the fight against cybercrime, protecting customers around the world by preventing breaches, eliminating fraud and protecting brands.