MOSCOW FORENSICS DAY '25



ALEXEY MOSKVICHEV

"APPLYING FORENSIC METHODS TO INVESTIGATE THEFTS COMMITTED WITH NFC TECHNOLOGY"

MKO SYSTEMS LLC

MFD

NFC IS A SHORT-RANGE WIRELESS COMMUNICATION TECHNOLOGY THAT USES RADIO-FREQUENCY IDENTIFICATION TO RECOGNIZE OBJECTS AND DEVICES AND TO READ STORED INFORMATION



Short-range communication



Fast pairing



Low power consumption



Versatile applications

IN 2025, THE NUMBER OF THEFTS USING NFC (OR CARDING) WORLDWIDE GREW MORE THAN THIRTY-FIVE TIMES COMPARED WITH 2024

Popular carding apps

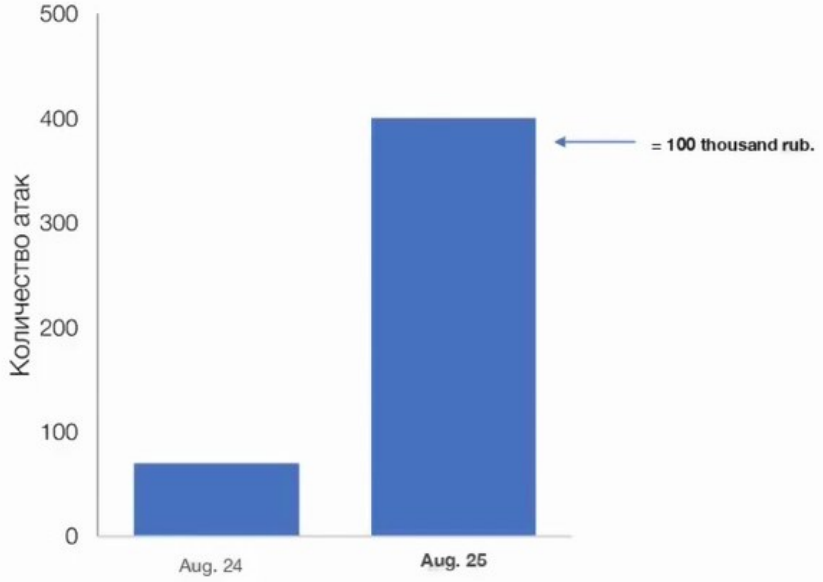
- NFCGate — relays NFC data from payment cards through compromised phones to fraudulently withdraw cash from ATMs.
- GhostTap — steals card data and loads it into digital wallets for contactless payments.
- SuperCard X — covertly collects bank card data and passes it on for fast illegal transactions.



IN RUSSIA IN 2025, MORE THAN 400 CASES OF CARDING VIA NFCGATE WERE RECORDED, WITH THE AVERAGE AMOUNT STOLEN AROUND 100 THOUSAND RUBLES

Frequently used criminal schemes:

- Classic scheme — the victim installs an app, holds up the card, enters the PIN — the fraudster with another device withdraws the money at an ATM.
- Reverse scheme — malware on the victim's phone relays the fraudster's card — the victim deposits money at an ATM, topping up the criminal's account.



IN RUSSIA IN 2025, MORE THAN 400 CASES OF CARDING VIA NFCGATE WERE RECORDED, WITH THE AVERAGE AMOUNT STOLEN AROUND 100 THOUSAND RUBLES

The app has several operating modes:

- Clone Mode — instant cloning and replay of the NFC signal on the device
- Relay Mode — remote relaying of the signal between several devices over the network
- Capture Mode — passive collection of data for analysis
- Replay Mode — replay of previously recorded NFC traffic of one of the devices that exchanged data in the selected session



NFCGATE IN ACTION: MAN-IN-THE-MIDDLE ATTACKS USING THE RELAY AND REPLAY MODES

Stages of an attack using NFCGate in its pure form:

- Social engineering
- Remote installation of NFCGate via a RAT (Remote Access Trojans)
- Setting up a connection between the victim's and the attacker's devices in Relay Mode
- Interception of the NFC data of the victim's card
- Obtaining the victim's PIN
- Reuse of the intercepted traffic via Replay Mode to steal money



NFCGate in Relay Mode on the attacker's side

NFCGate in Relay Mode on the victim's side

A NEW WAVE OF NFCGATE ATTACKS: MALICIOUS APK FILES EMULATING LEGITIMATE APPS OF BANKS OR GOVERNMENT AGENCIES

Modification of the NFCGate app involves:

- Changing the UI interface
- Hiding push notifications
- Changing package and app names
- Changing the format of the collected data
- Requesting the PIN of the victim's bank account when the app starts







CASE

INCIDENT OUTLINE (22.01.2025)

A call on Telegram from an unknown person posing as a law enforcement officer

Pretext: “Keeping the money safe”

Attacker's actions:

- A request to install an unknown app
- Instructions to launch it and hold a bank card up to the phone
- Advice to delete the app

Result: Withdrawal of 230,000 rub. from the card at an ATM by a third party

Subject of the examination: Redmi Note 11S mobile phone

DURING THE EXAMINATION A FILE “VTB (1).APK” WAS FOUND, DETECTED AS HEUR:TROJAN.ANDROIDOS.NFCGATE.A

Steps:

- MK Expert Plus → the “MTK Android” method
- Antivirus scan of the extracted data
- Identifying the suspicious file:
  - the file “VTB (1).apk” was found, with the modification date 22.01.2025 10:20
  - the threat type was identified — HEUR:Trojan.AndroidOS.NfcGate.a
  - the file's location — the directory the Telegram messenger uses to store received files and documents

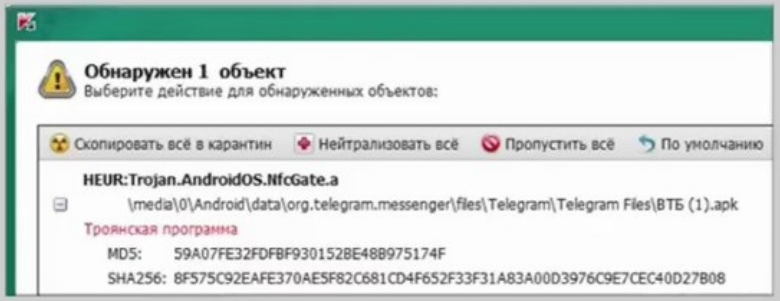


Fig. 1

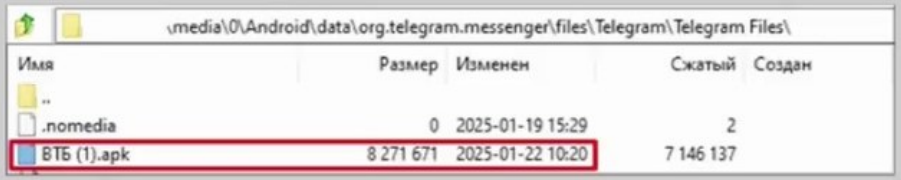


Fig. 2

TRACING HOW THE FILE “VTB (1).APK” REACHED THE DEVICE THROUGH THE FILE_TO_PATH.DB AND CACHE4.DB DATABASES OF THE TELEGRAM MESSENGER IN MK EXPERT PLUS

Steps:

- file_to_path.db → path_by_dialog_id → established the Telegram user ID 7****, from whom the file “VTB (1).apk” was received
- file_to_path.db → paths → established the ID 52****93 of the downloaded file “VTB (1).apk”
- qcache4.db → downloading_documents → by ID 52****93 the message receipt date 22.01.2025 10:20:44 was established, matching the modification date of the file “VTB (1).apk”
- qcache4.db → users → by ID 7**** the user name “1****” and the account name “ro****” were established



Fig. 3



Fig. 4

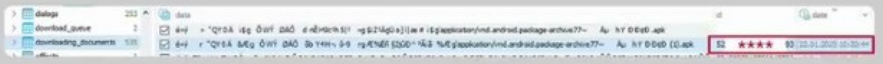


Fig. 5

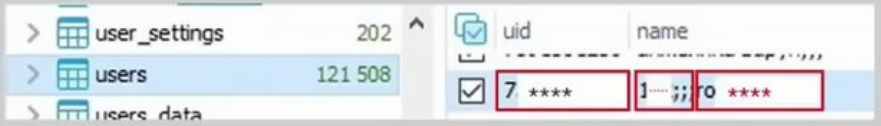


Fig. 6

ANALYSIS OF THE DECOMPILED CODE SHOWED THAT ITS FUNCTIONS (AND EVEN THE IDENTIFIER) MATCH THOSE OF THE LEGITIMATE NFCGATE APP

Steps:

- Manifest.xml contained the app identifier de.tu_darmstadt.seemoo.nfcgate with the name “VTB Protection”

Code comparison → the functions match the legitimate NFCGate app at https://github.com/nfcgate/nfcgate

- Discovery of the server address ***.***.***.**4 to which the intercepted NFC data was sent



Fig. 7



Fig. 8



Fig. 9



Fig. 10

FROM RECEIPT TO DELETION — A FORENSIC TIMELINE OF THE MALWARE

Steps:

- **portable_geller_**** @gmail.com.db →**
  geller_key_table in
  /data/data/com.google.android.googlequicksearchbox/
  databases
  contains the app installation history
  22.01.2025 10:33:18, 23.01.2025 11:15:41 and
  23.01.2025 11:17:19

LogToDump.log in
/data/user_de/0/
com.google.android.permissioncontroller/files
records two uninstalls: 23.01.2025 11:16 and
23.01.2025 11:41

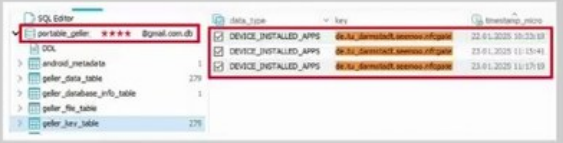


Fig. 11

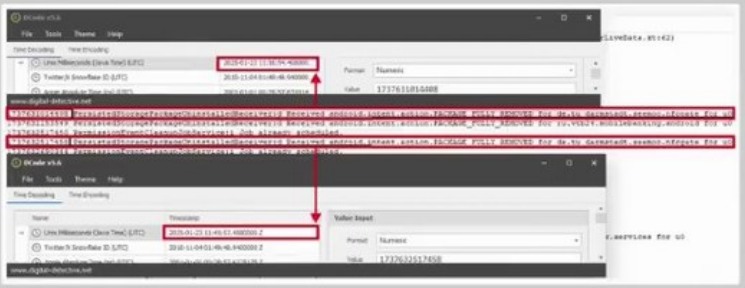


Fig. 12

FROM RECEIPT TO DELETION — A FORENSIC TIMELINE OF THE MALWARE

Steps:

- package-usage.list in /system/ contains information about the start of the com.android.nfc system service 23.01.2025 11:37

An image file recording a withdrawal of 230,000 rub. on 23.01.2025 14:39 in a directory linked to mobile banking confirmed the theft



Fig. 13

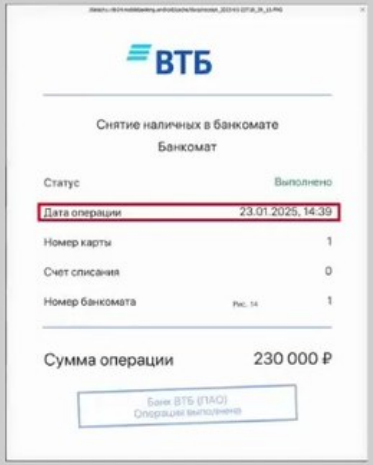


Fig. 14

SIMPLE RULES THAT WILL HELP PROTECT YOU FROM CARDING

- Install apps only from official stores (RuStore, Google Play)
- Do not give your CVV and PIN codes to strangers and do not enter them on suspicious sites or in apps
- If you receive a link to install or update a banking app, call the bank's hotline and check that the offer is genuine
- If the card is compromised, block it at once through the hotline or the banking app





The financial abyss is the deepest of all abysses, you can fall into it all your life.

O. Bender