MOSCOW FORENSICS DAY ‘25

АЛЕКСЕЙ МОСКВИЧЕВ

«ПРИМЕНЕНИЕ МЕТОДОВ ФОРЕНЗИКИ ПО РАССЛЕДОВАНИЮ ХИЩЕНИЙ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ NFC»

ООО «МКО СИСТЕМЫ»

MFD

NFC — ЭТО ТЕХНОЛОГИЯ БЕСПРОВОДНОЙ СВЯЗИ МАЛОГО РАДИУСА ДЕЙСТВИЯ, ИСПОЛЬЗУЮЩАЯ РАДИОЧАСТОТНУЮ ИДЕНТИФИКАЦИЮ ДЛЯ РАСПОЗНАВАНИЯ ОБЪЕКТОВ, УСТРОЙСТВ И СЧИТЫВАНИЯ СОХРАНЕННОЙ ИНФОРМАЦИИ

Связь на короткие расстояния

Быстрое сопряжение

Низкое энергопотребление

Универсальные приложения

В 2025 ГОДУ ПО ВСЕМУ МИРУ ЧИСЛО СЛУЧАЕВ ХИЩЕНИЙ С ИСПОЛЬЗОВАНИЕМ NFC (ИЛИ КАРДИНГА) ВЫРОСЛО БОЛЕЕ ЧЕМ В ТРИДЦАТЬ ПЯТЬ РАЗ ПО СРАВНЕНИЮ С 2024 ГОДОМ

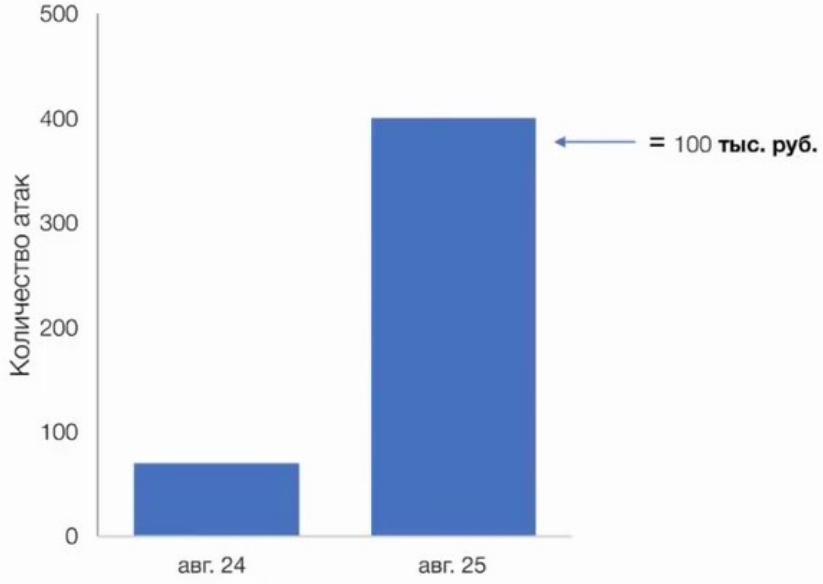
Популярные приложения для кардинга

- **NFCGate** — передает данные NFC с платежных карт через взломанные телефоны для мошеннического снятия наличных в банкоматах.
- **GhostTap** — крадет данные карт и загружает их в цифровые кошельки для бесконтактных платежей.
- **SuperCard X** — скрытно собирает данные банковских карт и передает их для проведения быстрых незаконных транзакций.

В РОССИИ В 2025 ГОДУ ЗАФИКСИРОВАНО БОЛЕЕ 400 СЛУЧАЕВ КАРДИНГА С ПОМОЩЬЮ NFCGATE, ПРИ ЭТОМ СРЕДНЯЯ СУММА ХИЩЕНИЙ СОСТАВЛЯЛА ОКОЛО 100 ТЫСЯЧ РУБЛЕЙ

Часто используемые преступные схемы:

- **Классическая схема** — жертва устанавливает приложение, прикладывает карту, вводит PIN — мошенник с другим устройством снимает деньги у банкомата.
- **Обратная схема** — вредонос на телефоне жертвы ретранслирует карту мошенника — жертва вносит деньги в банкомат, пополняя счет злоумышленника.



В РОССИИ В 2025 ГОДУ ЗАФИКСИРОВАНО БОЛЕЕ 400 СЛУЧАЕВ КАРДИНГА С ПОМОЩЬЮ NFCGATE, ПРИ ЭТОМ СРЕДНЯЯ СУММА ХИЩЕНИЙ СОСТАВЛЯЛА ОКОЛО 100 ТЫСЯЧ РУБЛЕЙ

Приложение имеет несколько режимов работы:

- **Clone Mode** — моментальное клонирование и воспроизведение NFC-сигнала на устройстве
- **Relay Mode** — удаленная ретрансляция сигнала между несколькими устройствами по сети
- **Capture Mode** — пассивный сбор данных для анализа
- **Replay Mode** — повторное воспроизведение ранее записанного NFC-трафика одного из устройств, между которыми производился обмен данными выбранной сессии

NFCGATE В ДЕЙСТВИИ: АТАКИ ТИПА MAN-IN-THE-MIDDLE («ЧЕЛОВЕК ПОСЕРЕДИНЕ») С ИСПОЛЬЗОВАНИЕМ РЕЖИМОВ RELAY И REPLAY

Этапы атаки с использованием NFCGate в чистом виде:

- Социальная инженерия
- Удаленная установка NFCGate через RAT (Remote Access Trojans — трояны удаленного доступа)
- Установка соединения между устройствами жертвы и злоумышленника в режиме **Relay Mode**
- Перехват NFC-данных карты жертвы
- Получение PIN-кода жертвы
- Повторное использование перехваченного трафика с помощью режима **Replay Mode** для кражи денег

NFCGate в режиме Relay Mode на стороне атакующего

NFCGate в режиме Relay Mode на стороне жертвы

НОВАЯ ВОЛНА АТАК NFCGATE: ИСПОЛЬЗОВАНИЕ ВРЕДОНОСНЫХ APK-ФАЙЛОВ, ЭМУЛИРУЮЩИХ РАБОТУ ЛЕГИТИМНЫХ ПРИЛОЖЕНИЙ БАНКОВ ИЛИ ГОСУДАРСТВЕННЫХ СТРУКТУР

Модификация приложения NFCGate предусматривает:

- Смену UI-интерфейса
- Сокрытие push-уведомлений
- Смену имен пакетов, приложений
- Смену формата собираемых данных
- Запрос PIN-кода банковского счета жертвы при запуске приложения

КЕЙС

СХЕМА ИНЦИДЕНТА (22.01.2025 г.)

Звонок в Telegram от неизвестного, представившегося сотрудником правоохранительных органов

Легенда: «Сохранение денежных средств»

Действия злоумышленника:

- Просьба установить неизвестное приложение
- Инструкция запустить его и приложить к телефону банковскую карту
- Рекомендация удалить приложение

Результат: Снятие 230 000 руб. с карты через банкомат третьим лицом

Предмет экспертизы: Мобильный телефон Redmi Note 11S

В ХОДЕ ПРОИЗВОДСТВА ЭКСПЕРТИЗЫ ОБНАРУЖЕН ФАЙЛ «ВТБ (1).APK», КОТОРЫЙ ОПРЕДЕЛЯЕТСЯ КАК HEUR:TROJAN.ANDROIDOS.NFCGATE.A

Шаги:

- МК Эксперт Плюс → метод «MTK Android»
- Антивирусное сканирование извлеченных данных
- Выявление подозрительного файла:
  - найден файл **«ВТБ (1).apk»** с датой изменения **22.01.2025 10:20**
  - определен тип угрозы — **HEUR:Trojan.AndroidOS.NfcGate.a**
  - местоположение файла — каталог, используемый мессенджером **Telegram** для хранения полученных файлов и документов

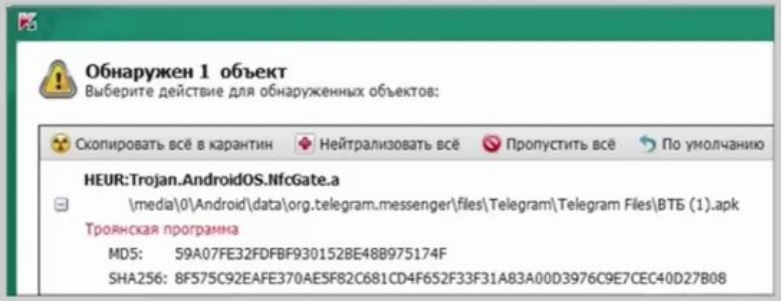


Рис. 1

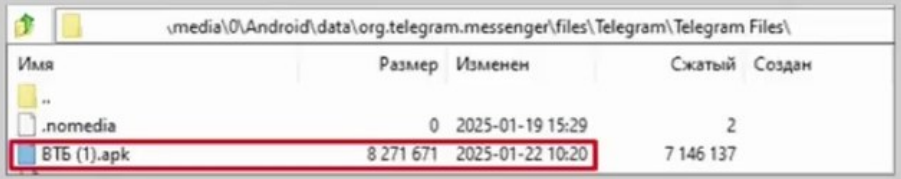


Рис. 2

ОТСЛЕЖИВАНИЕ ПУТИ ПОСТУПЛЕНИЯ ФАЙЛА «ВТБ (1).APK» НА УСТРОЙСТВО ПО БАЗАМ ДАННЫХ FILE_TO_PATH.DB И CACHE4.DB МЕССЕНДЖЕРА TELEGRAM В ПО «МК ЭКСПЕРТ ПЛЮС»

Шаги:

- **file_to_path.db** → **path_by_dialog_id** → установлен ID пользователя Telegram **7******, от которого получен файл «ВТБ (1).apk»
- **file_to_path.db** → **paths** → установлен идентификатор **52****93** загруженного файла «ВТБ (1).apk»
- **qcache4.db** → **downloading_documents** → по идентификатору 52****93 установлена дата получения сообщения **22.01.2025 10:20:44**, которая совпадает с датой изменения файла «ВТБ (1).apk»
- **qcache4.db** → users → по ID 7**** установлены имя пользователя «**1******» и имя его учетной записи «**ro******»

Рис. 3

Рис. 4

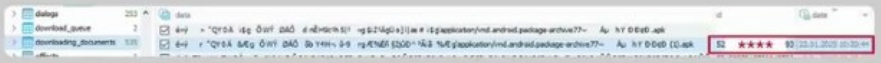


Рис. 5

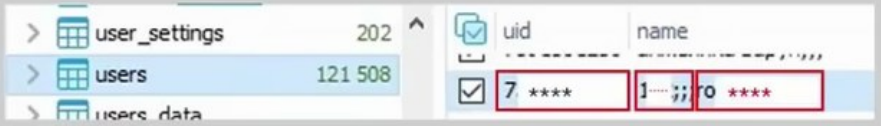


Рис. 6

АНАЛИЗ ДЕКОМПИЛИРОВАННОГО КОДА ПОКАЗАЛ, ЧТО ЕГО ФУНКЦИИ (И ДАЖЕ ИДЕНТИФИКАТОР) СОВПАДАЮТ С ФУНКЦИЯМИ ЛЕГИТИМНОГО ПРИЛОЖЕНИЯ NFCGATE

Шаги:

- В **Manifest.xml** найден идентификатор приложения **de.tu_darmstadt.seemoo.nfcgate** с именем «Защита ВТБ»
- Сравнение кода → **функции совпадают** с легитимным приложением NFCGate на https://github.com/nfcgate/nfcgate
- Обнаружение **адреса сервера** ***.***.***.**4, на который отправлялись перехваченные NFC-данные

Рис. 7

Рис. 8

Рис. 9

Рис. 10

ОТ ПОЛУЧЕНИЯ ФАЙЛА ДО УДАЛЕНИЯ — FORENSIC-ТАЙМЛАЙН ВРЕДОНОСА

Шаги:

- **portable_geller_**** @gmail.com.db** → **geller_key_table** в /data/data/com.google.android.googlequicksearchbox/databases содержит историю **установки** приложения **22.01.2025 10:33:18, 23.01.2025 11:15:41** и **23.01.2025 11:17:19**

- **LogToDump.log** в /data/user_de/0/com.google.android.permissioncontroller/files фиксирует два **удаления: 23.01.2025 11:16** и **23.01.2025 11:41**

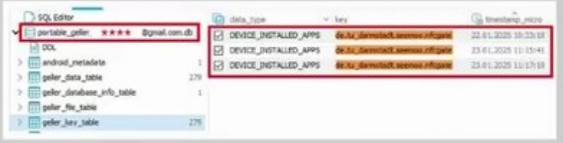


Рис. 11

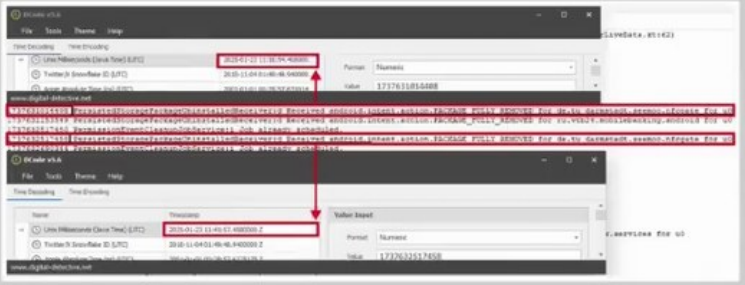


Рис. 12

ОТ ПОЛУЧЕНИЯ ФАЙЛА ДО УДАЛЕНИЯ — FORENSIC-ТАЙМЛАЙН ВРЕДОНОСА

Шаги:

- **package-usage.list** в каталоге /system/ содержит информацию о запуске системной службы com.android.nfc **23.01.2025 11:37**

- **Графический файл** с записью о снятии **230 000 руб. 23.01.2025 14:39** в каталоге, связанном с мобильным банкингом, подтвердил факт хищения

Рис. 13

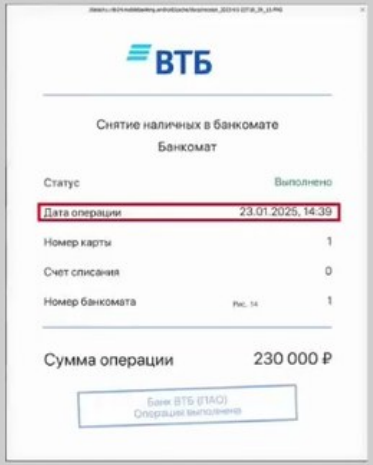


Рис. 14

ПРОСТЫЕ ПРАВИЛА, КОТОРЫЕ ПОМОГУТ ЗАЩИТИТЬСЯ ОТ КАРДИНГА

- Устанавливайте приложения только из официальных магазинов (RuStore, Google Play)
- Не сообщайте CVV- и PIN-коды посторонним и не вводите их на подозрительных сайтах или в приложениях
- При получении ссылки на установку или обновление банковского приложения позвоните на горячую линию банка и уточните подлинность предложения
- Если карта скомпрометирована, сразу заблокируйте ее через горячую линию или банковское приложение

Финансовая пропасть — самая глубокая из всех пропастей, в нее можно падать всю жизнь.

О. Бендер