GROUP IB

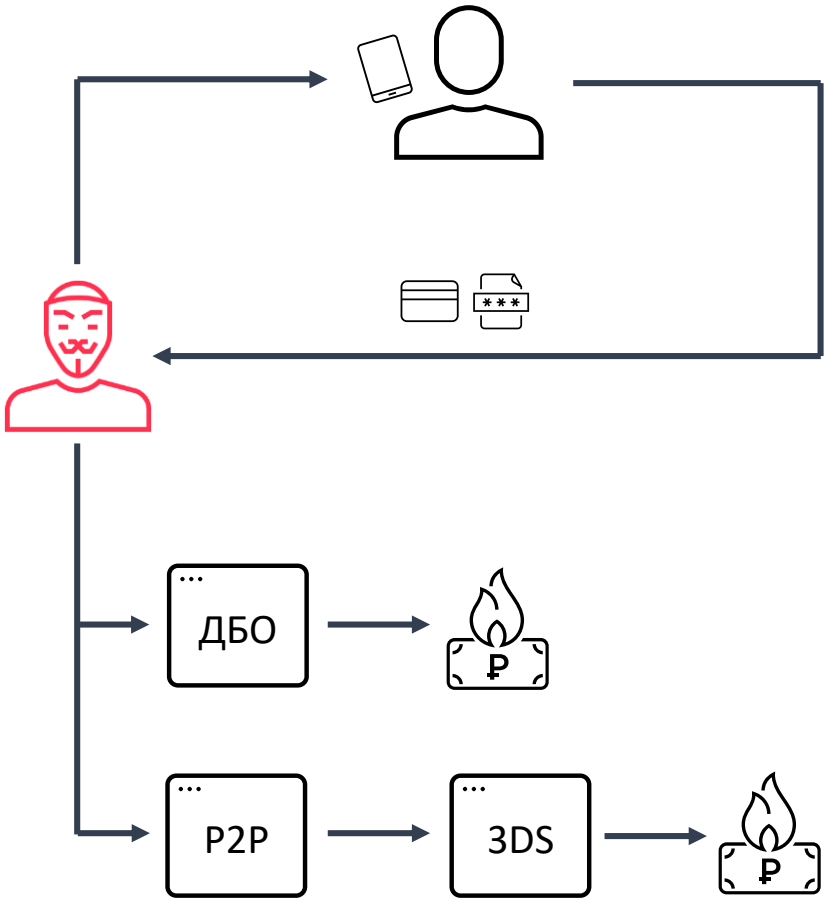
# Quid pro quo

Соц. инженерия: кейсы, противодействие, тренды.

**Павел Крылов**

Руководитель направления по противодействию онлайн-мошенничеству

# Выманивание логина/пароля/карты/OTP




**Kill chain:**

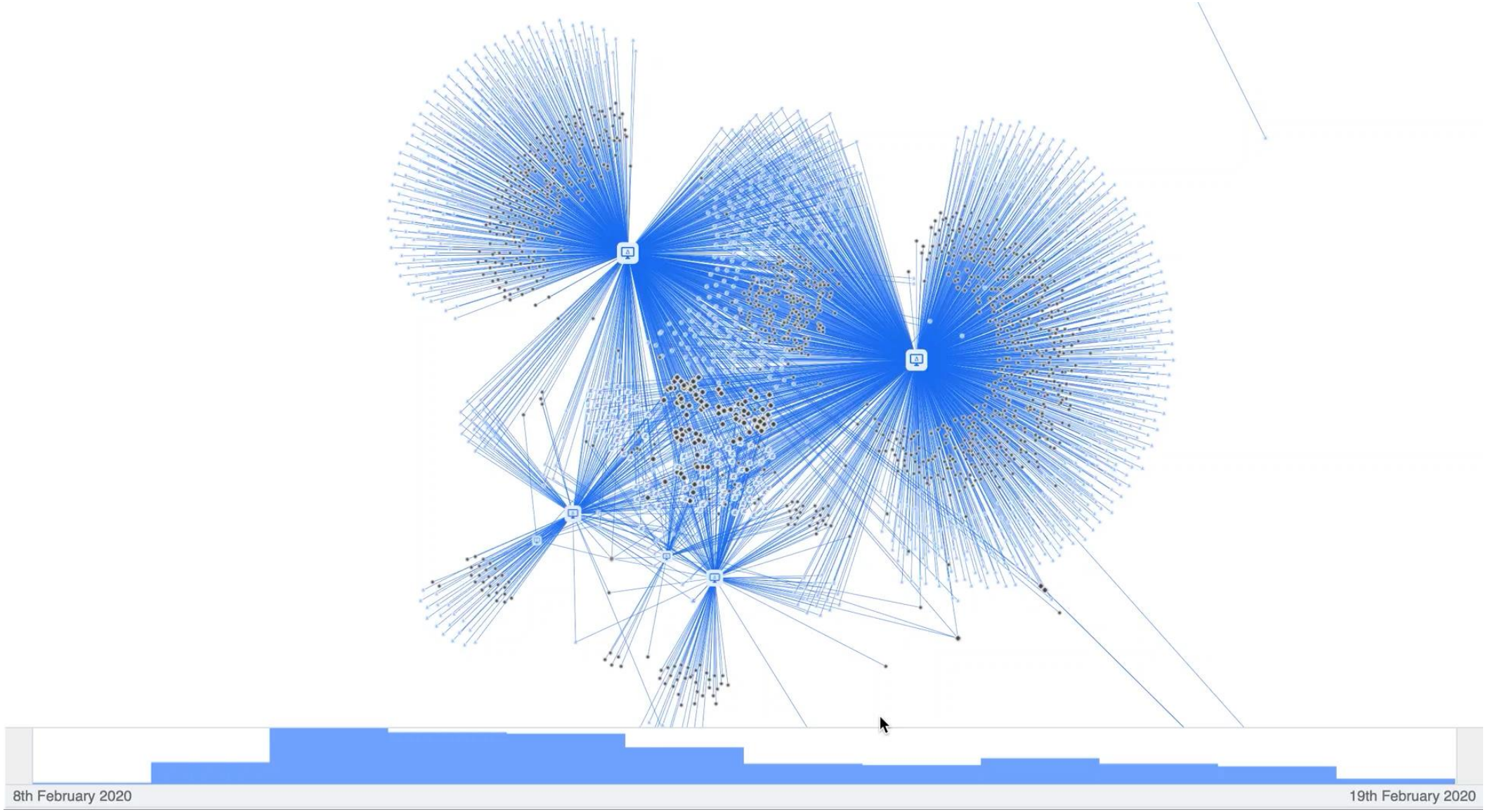
- Мошенник с использованием соц. инженерии получает доступ в ДБО или реквизиты карты
- Проходит перерегистрацию в ЛК
- Похищает полученные средства

**Выявление:**

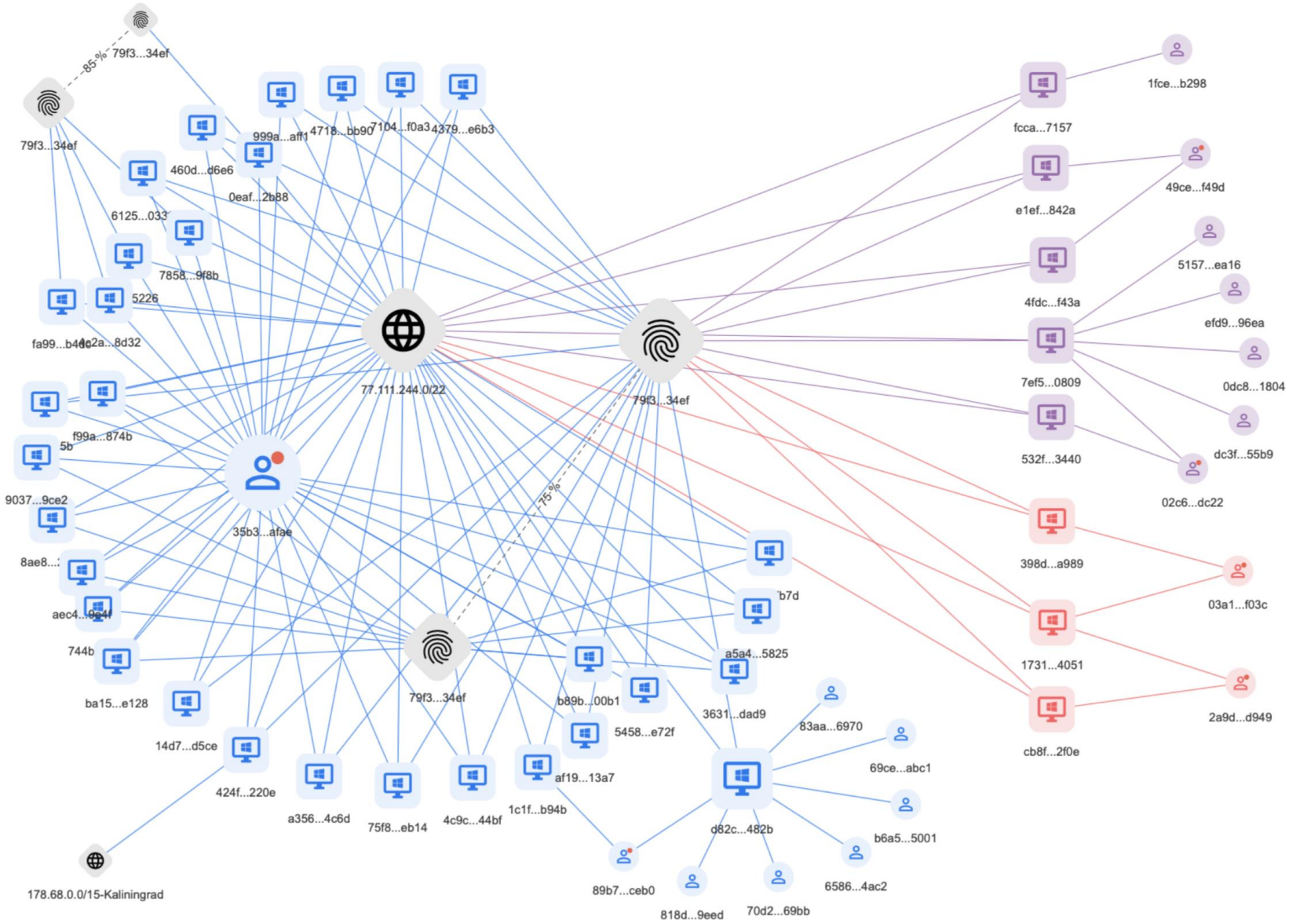
- **Система поведенческой аналитики:**
  a. **Нетипичное устройство клиента**
  b. **перерегистрация (или первичная регистрация)**
  c. наличие **связей с инцидентами**

- **На стороне банка: нетипичная** операция с **не доверенного устройства,** уже известный счет получателя-мошенника

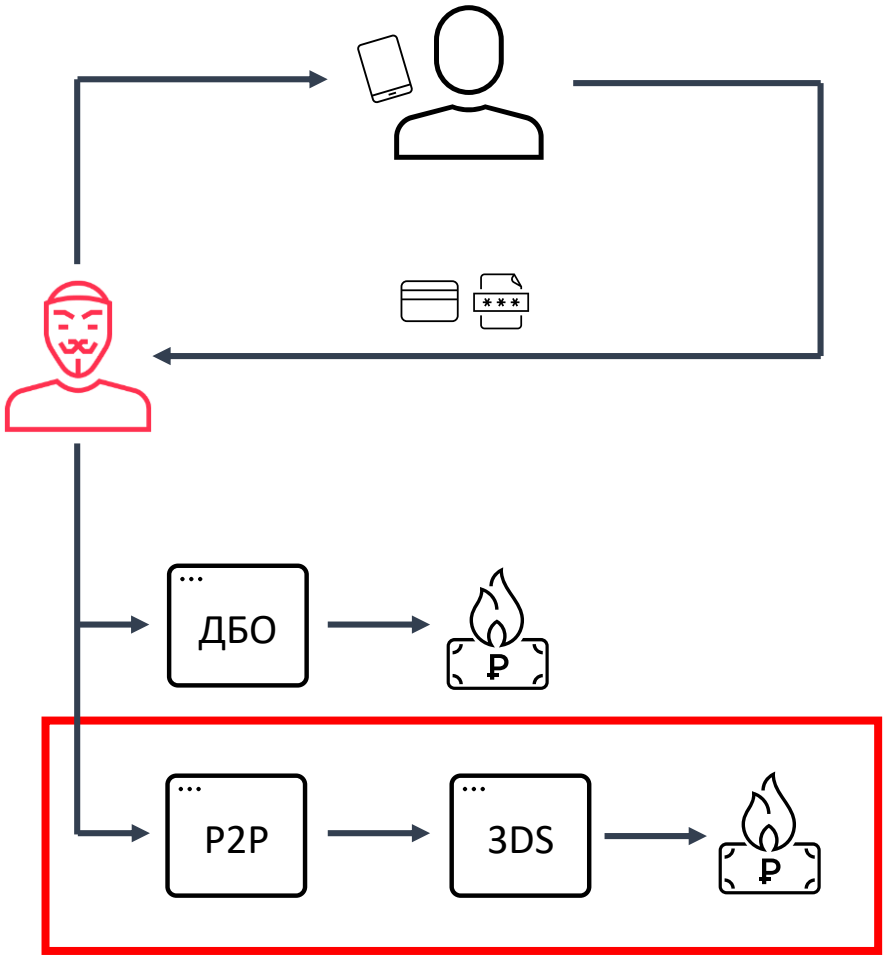
# Выманивание логина/пароля/карты/OTP



# Выманивание логина/пароля/карты/OTP



# Выманивание логина/пароля/карты/OTP




**Статистика ФинЦЕРТ 2019:**

- 371,1 тыс. мошеннических CNP-транзакций
- 2971,3 млн. руб. сумма ущерба
- банки возмещают каждый 5-й похищенный рубль

**Сложности:**

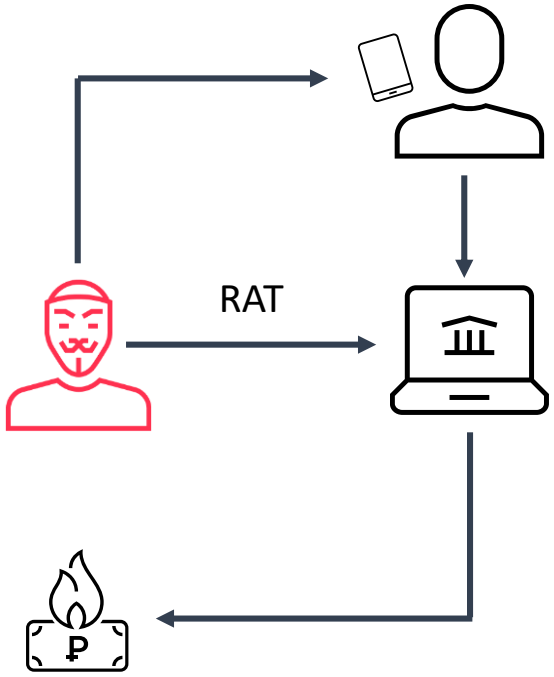
- Много способов и каналов реализации CNP-мошенничества: p2p, кошельки, покупка товаров/услуг, bitcoin
- Они не подконтрольны эмитенту

**Решение:**

- Анализ типичности устройства для карты при подтверждении платежа на 3DS
- Выявление множественных подтверждений по разным картам с одного устройства

# «Прозвонщики/удаленщики»

**декабрь 2018 – апрель 2019**




**Kill chain:**

- Мошенник с использованием IP-телефонии и подменой номера представляется «сотрудником» банка
- Просят поставить RAT под различными предлогами
- Переводят средства через удаленное управление

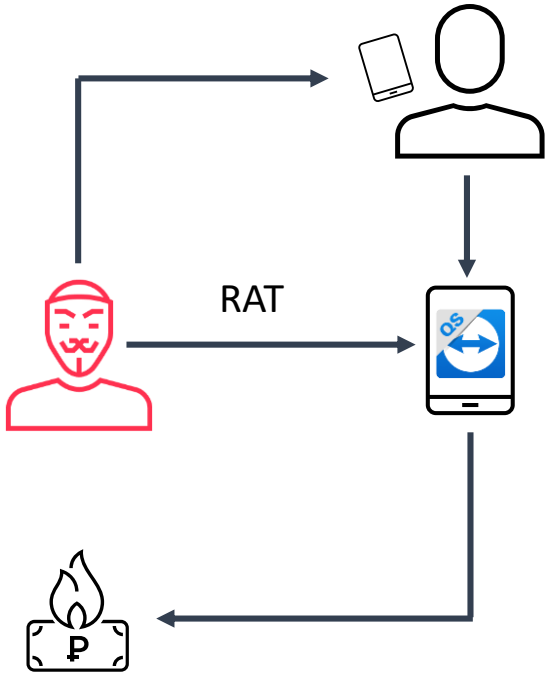
**Выявление:**

- **Система поведенческой аналитики:**
  a. **Использование RAT при работе в приложении**
  b. **Схожесть сценария работы пользователя с известными случаями работы мошенника**
  c. **Аномальное поведение пользователя**

- **На стороне банка: нетипичная** операция или перевод на уже известный счет мошенника

# «Прозвонщики/удаленщики»

**май 2019 – по настоящий момент**




**Kill chain:**

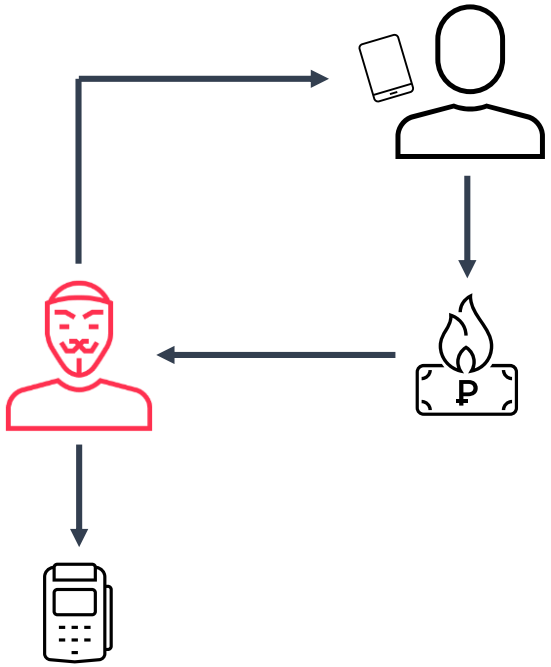
- Мошенник с использованием IP-телефонии и подменой номера представляется «сотрудником» банка
- Просят поставить RAT под различными предлогами
- Переводят средства через удаленное управление

**Выявление:**

- **Система поведенческой аналитики:**
  a. **Использование RAT при работе в приложении**
  b. **Схожесть сценария работы пользователя с известными случаями работы мошенника**
  c. **Аномальное поведение пользователя**

- **На стороне банка: нетипичная** операция или перевод на уже известный счет мошенника

# «Чистая» социалка



**Kill chain:**

- Мошенник вводит в заблуждение жертву
- Жертва сама переводит мошеннику деньги
- Мошенник как правило использует банкомат для снятия средств

**Выявление:**

- **На стороне банка:** **нетипичная** операция или перевод на уже известный счет мошенника

**Статистика:**

- Кардинально разнится от банка к банку
- От 5 до 60% таких случаев

# Новый «конкурент»

**Kill chain:**

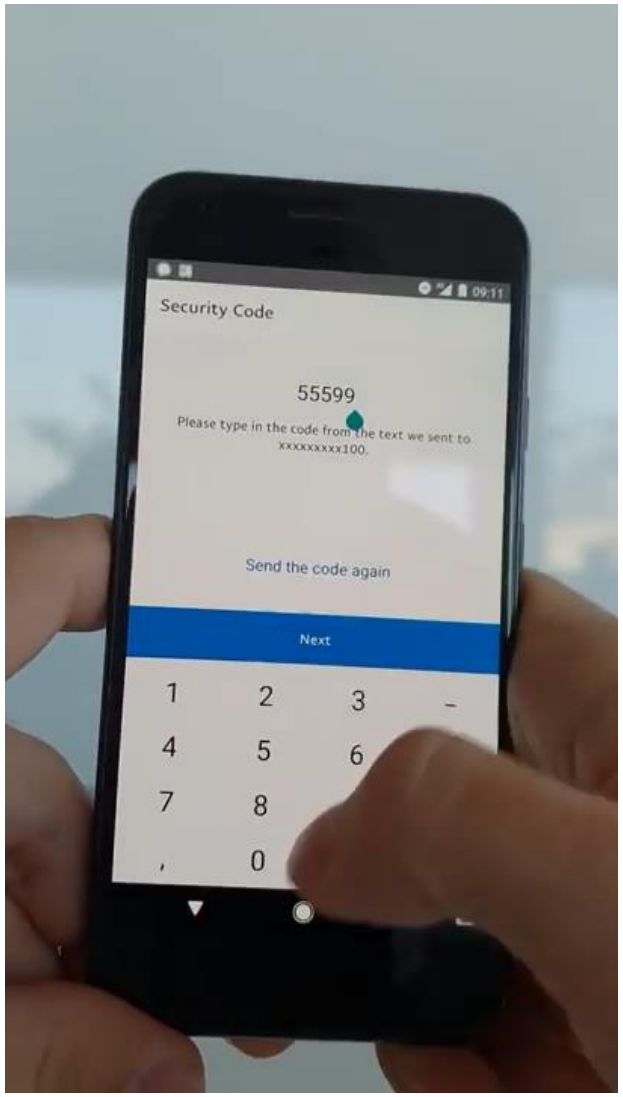
- Фишинговая рассылка, установка мобильного ВПО
- Клиент самостоятельно входит в приложение по ПИН-коду, отпечатку пальца и т.п.
- ВПО вместо пользователя кликает в приложении с использованием Accessibility Service

**Выявление:**

- **Система поведенческой аналитики:**
  a. **Действия в приложении через Accessibility Service**

- **На стороне банка:** **нетипичная** операция или на уже известный счет получателя-мошенника

https://www.youtube.com/watch?v=yn04eLoivX8



# Тенденции

## Рост количества и объема

Малый процент банков полноценно используют второй обязательный признак совершения операции без согласия клиента

## Рост «чистой» социалки

По мере расширения арсенала технологий борьбы с соц. инженерией, банки все больше будут «выталкивать» мошенника на «чистую» социалку.

## Лидером будет CNP-fraud

Процент проникновения 3DS 2.x невелик, как и использование его принципов в 3DS 1.x.

## «Автозалив» в моб. канале

Может составить конкуренцию текущим методам хищения с использованием соц. инженерии.

# Предотвращаем и расследуем киберпреступления с 2003 года

**Павел Крылов**

Руководитель направления по противодействию онлайн-мошенничеству

www.group-ib.ru
info@group-ib.com
twitter.com/groupib
t.me/group_ib
group-ib.ru/blog
+7 495 984 33 64
facebook.com/groupib
instagram.com/group_ib