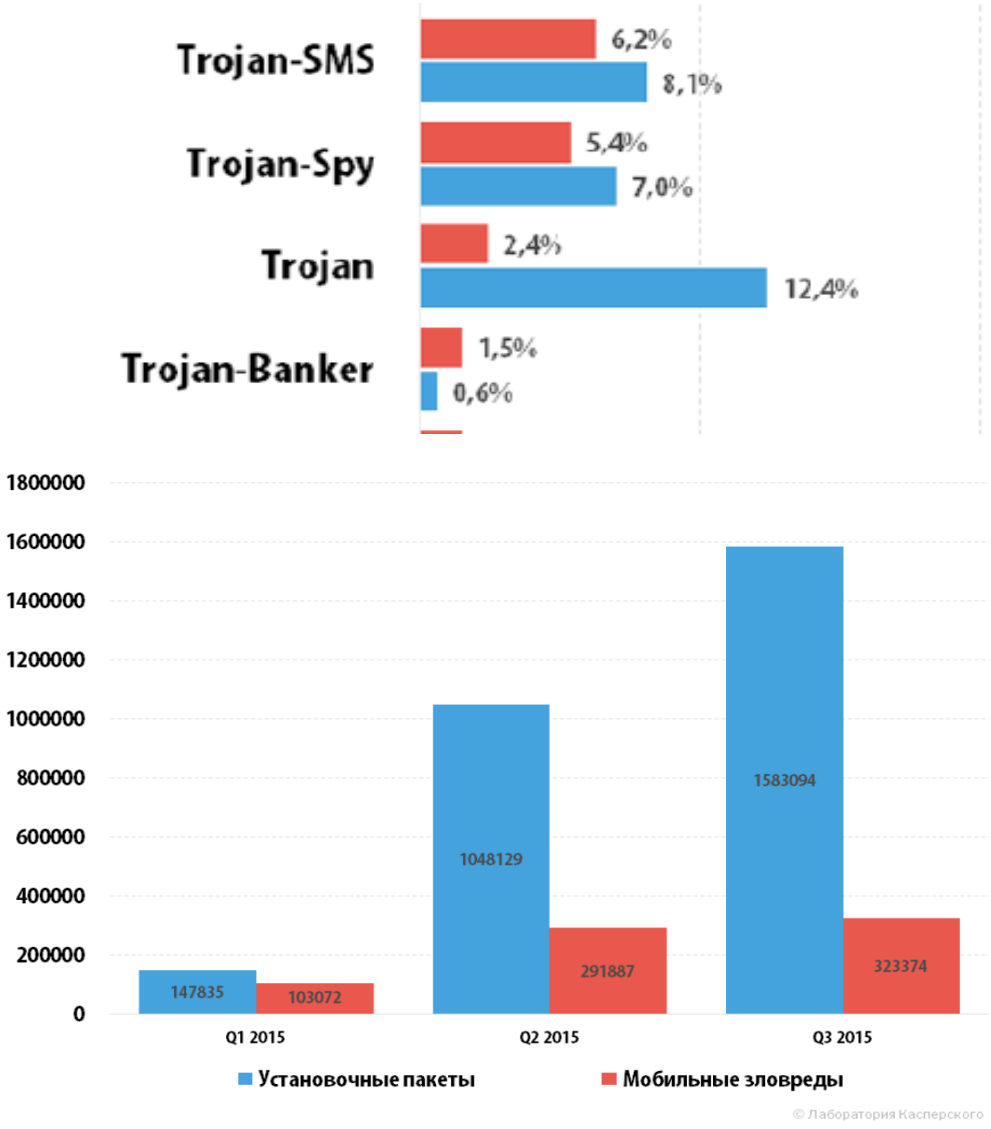
# Практические вопросы противодействия мошенничеству в каналах ДБО

Денис Камзеев, CISSP
Начальник отдела ИБ
Управления экономической безопасности
АО «Райффайзенбанк»

- **Информационные угрозы в финансовом секторе**
- **Электронное мошенничество 2015. Взгляд со стороны Банка**
- **Практика противодействия**

# Информационные угрозы в финансовом секторе *




*Количество обнаруженных вредоносных установочных пакетов и новых мобильных угроз (Q1 2015 – Q3 2015)*

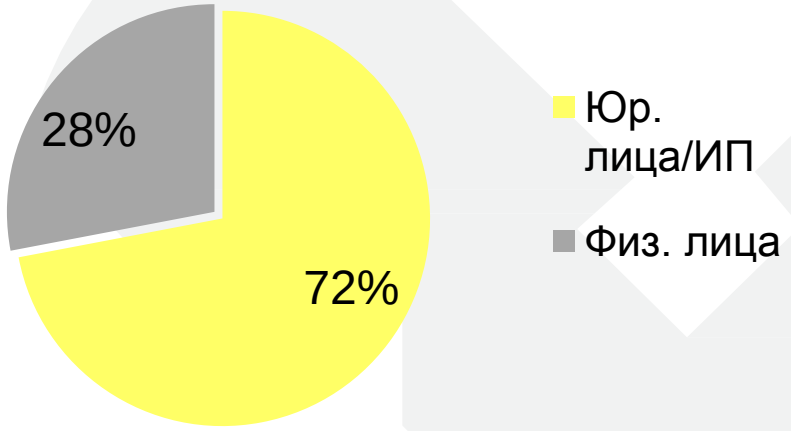
- Мобильные троянские программы
- Банковские троянские программы, APT
- Логические атаки на ATM и POS
- DDoS

*использованы данные Kaspersy Lab, Group-IB, Positive Technologies

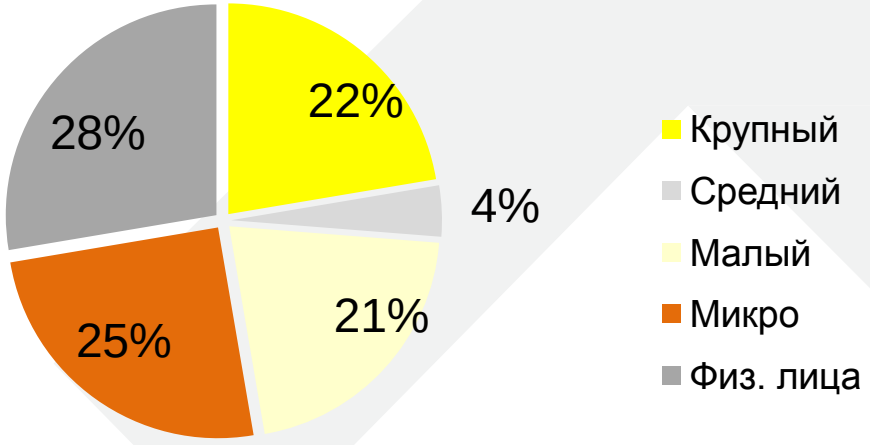
# Электронное мошенничество. Результаты и тренды 2015

- **Снижение активности мошенников** в отношении систем интернет-банкинга и мобильного банка **для физических лиц**.
- **99.99%** объема мошеннических операций в 2015 году – платежи юр.лиц и ИП.
- **«Таргетирование».** Характерная тенденция для 2015 года - избирательность при подготовке и проведении атаки. Не все пользователи одинаково интересны с точки зрения мошенничества.

**Цели злоумышленников, ФЛ/ЮЛ %**




**Цель злоумышленников, сегмент, %**

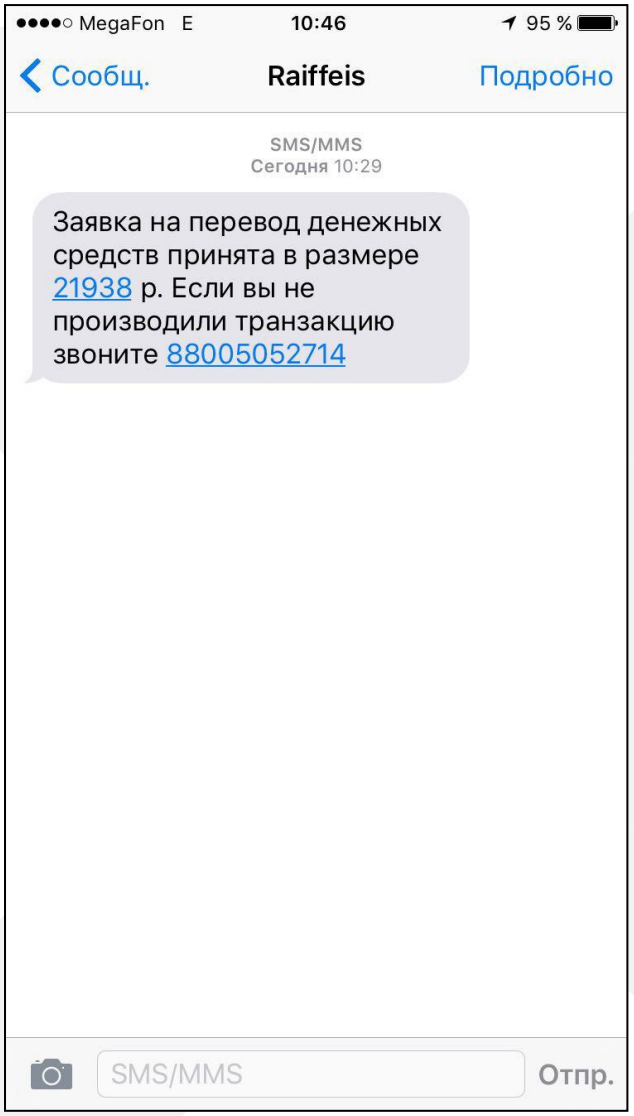


# Электронное мошенничество. Результаты и тренды 2015

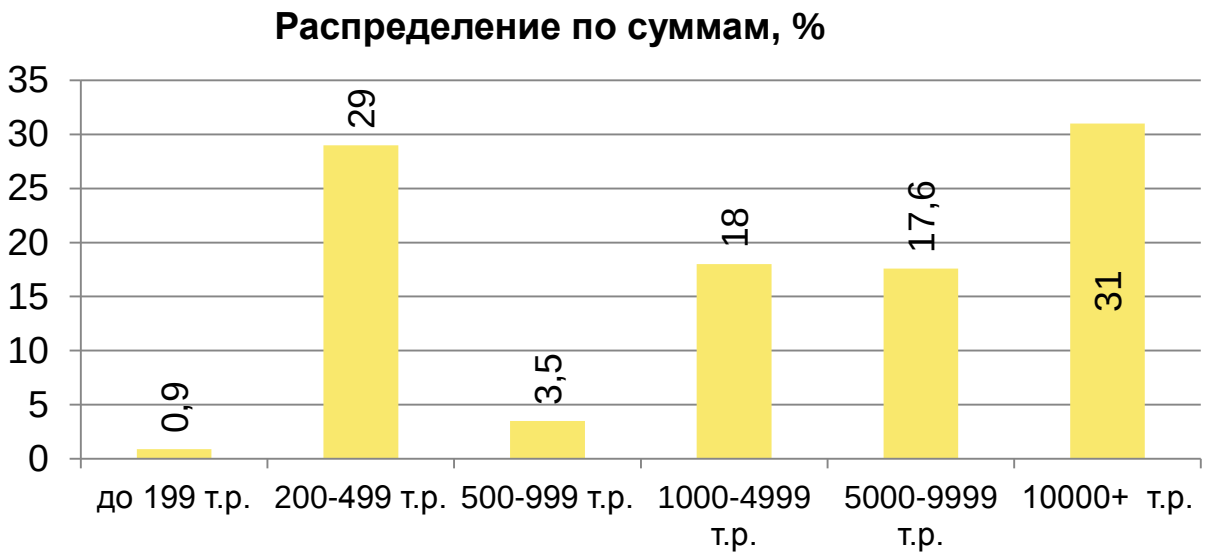
- **Уверенный рост количества зараженных мобильных устройств** в отсутствие явного увеличения атак на мобильный банкинг – потенциальная площадка для будущего мошенничества.

- Увеличение количества и рост мощности DDoS атак. Доступность и простота организации атак до 90 Gbps.

- **Социальная инженерия** по прежнему остается одним из главных инструментов для контакта с жертвой. Цель - последующая компрометация конечного устройства, либо непосредственное выполнение мошеннических транзакций



# Электронное мошенничество. Результаты и тренды 2015





- 78% мошеннических платежей в ДБО находится в диапазоне 200-500 тыс.р.
- Использование различных тактик. Таргетирование потенциальной жертвы подразумевает изучение поведения, выбор метода мошенничества, наиболее похожего на «нормальное» поведение клиента. Типичный пример – «зарплатная ведомость» в последний рабочий день месяца.

# Электронное мошенничество в ДБО. Основные векторы атак

- Интернет-банкинг. По прежнему наиболее востребованный канал ДБО, с точки зрения мошенничества. Компрометация клиентского устройства – наиболее распространённая причина мошенничества.

- Мобильный банкинг. Такие методы как фишинг, распространение вредоносного ПО через рекламу в мобильных приложениях, возможность установки приложений для Android из любого источника, а не из официального каталога Google Play, используются злоумышленниками для инфицирования и компрометации клиентского мобильного устройства.

- Используя методы социальной инженерии, мошенники осуществляют звонки или SMS-рассылки от имени "банка" для получения конфиденциальных данных клиента (таких как логин, пароль, одноразовый код подтверждения платежа, данные кредитной карты).

- Не технические методы. Поддельная доверенность, получение SIM карты, привязанной к мобильному номеру телефона жертвы. Поддельный паспорт.

# О практике противодействия

**Технические меры** обеспечения безопасности ДБО и противодействия мошенничеству

- Мониторинг транзакций. Использование максимально доступного количества параметров платежа – как финансовых, так и технических (user agent, fingerprinting) с регулярным пересмотром и корректировкой действующей модели обнаружения.
- Двухфакторная и out-of-band авторизация платежей
- White box penetration test
- Анализ защищенности кода – неотъемлемая часть процесса разработки
- Анализ рисков функциональности ДБО на стадии разработки требований, бизнес идеи.
- Наличие гибкого механизма лимитов на проведение операций, в зависимости от категории клиента и типа операции

# О практике противодействия

**Организационные меры**

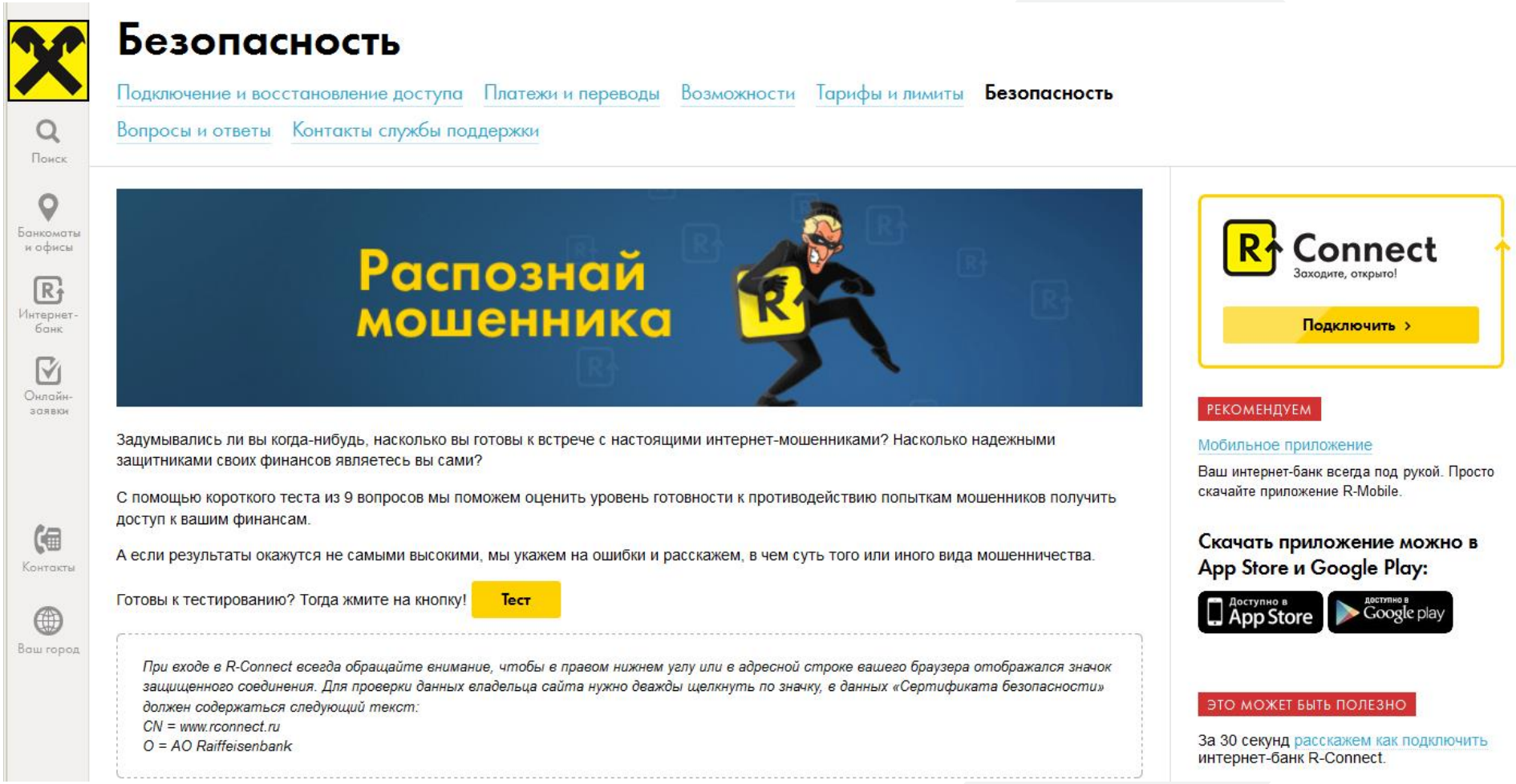
- Постоянное повышение осведомленности сотрудников Банка, непосредственно взаимодействующих с клиентами.

- Проведение практических тренингов по безопасной разработке.

- Повышение осведомленности клиентов. Продвижение материалов, фокусирующих клиента на вопросах безопасности. Онлайн курсы (http://www.raiffeisen.ru/retail/remote_service/connect/security/).

# О практике противодействия

http://www.raiffeisen.ru/retail/remote_service/connect/security/



# СПАСИБО ЗА ВНИМАНИЕ !


# ВОПРОСЫ?