A large, stylized yellow graphic on the right side of the slide, resembling a jagged, abstract shape or a stylized letter 'M' with a curved top. It is composed of thick yellow lines.

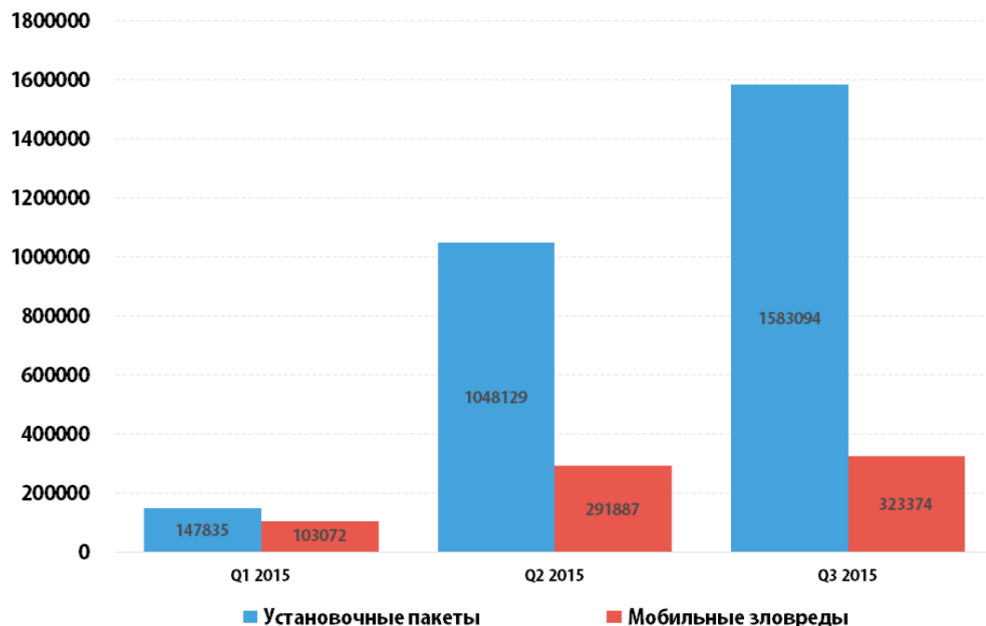
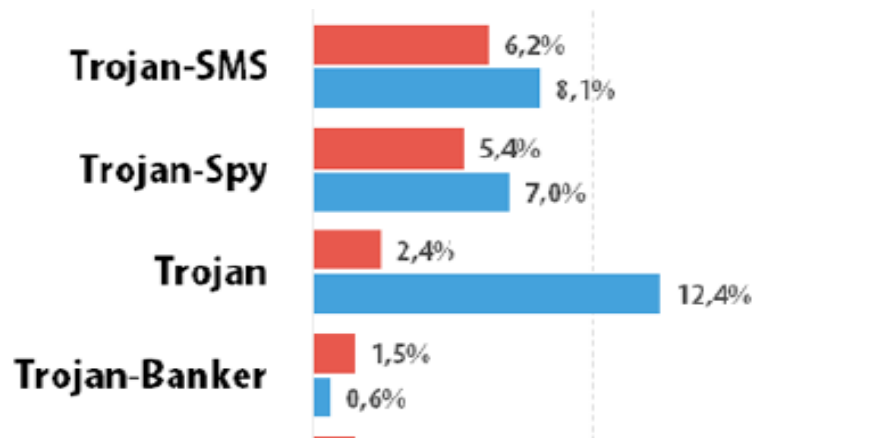
Практические вопросы противодействия мошенничеству в каналах ДБО

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 *



© Лаборатория Касперского

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

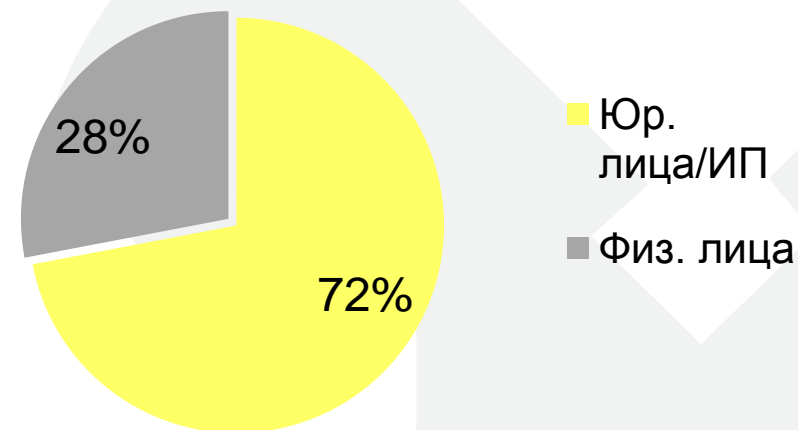
- Мобильные троянские программы
- Банковские троянские программы, АРТ
- Логические атаки на АТМ и POS
- DDoS

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

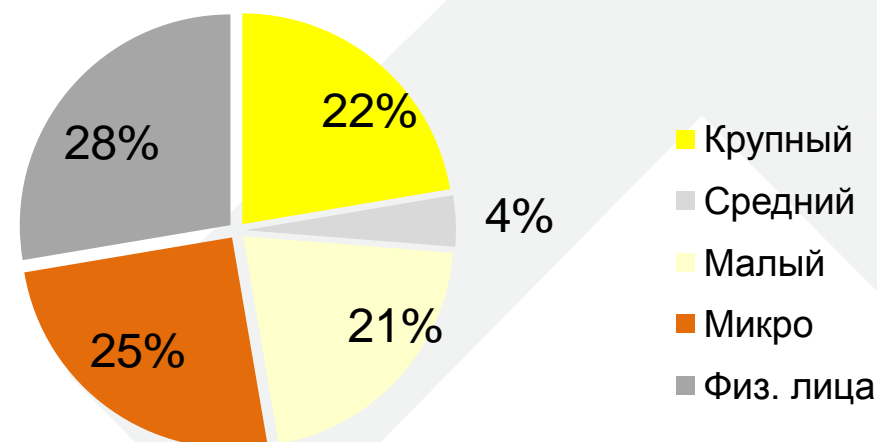
Электронное мошенничество. Результаты и тренды 2015

- **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 %

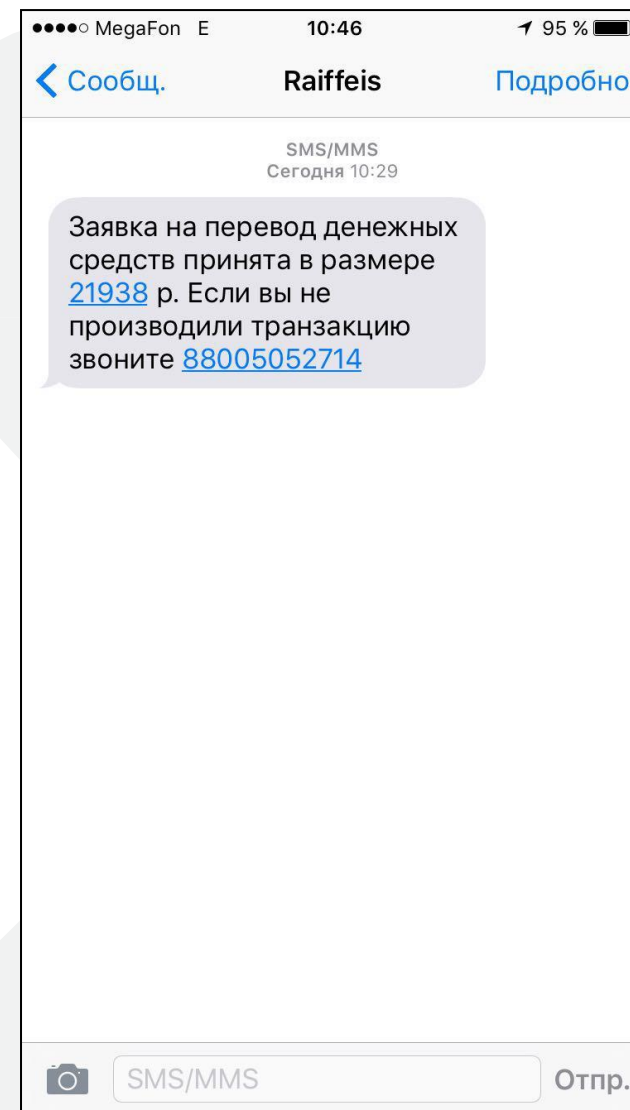


Цель злоумышленников, сегмент, %



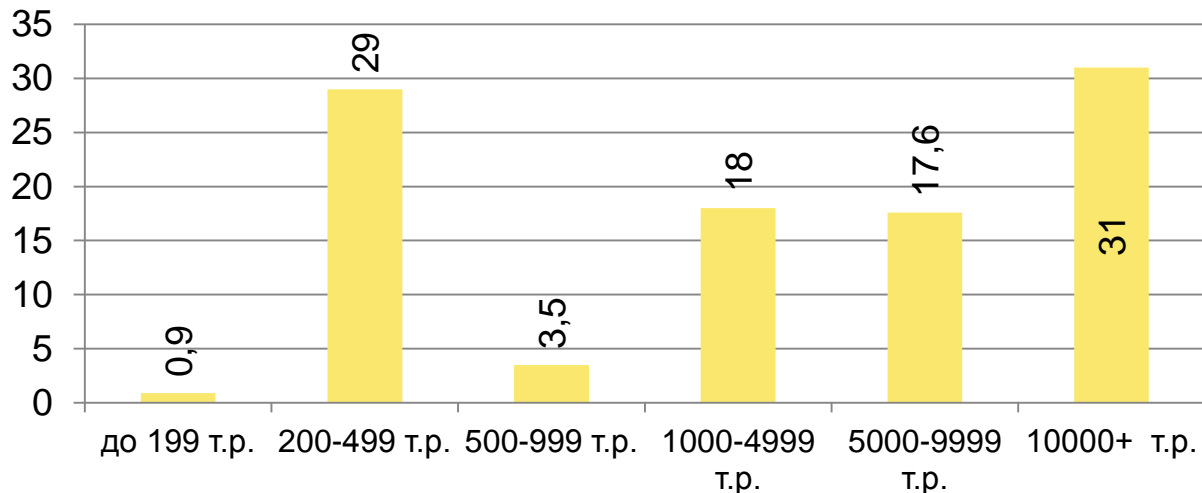
Электронное мошенничество. Результаты и тренды 2015

- **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

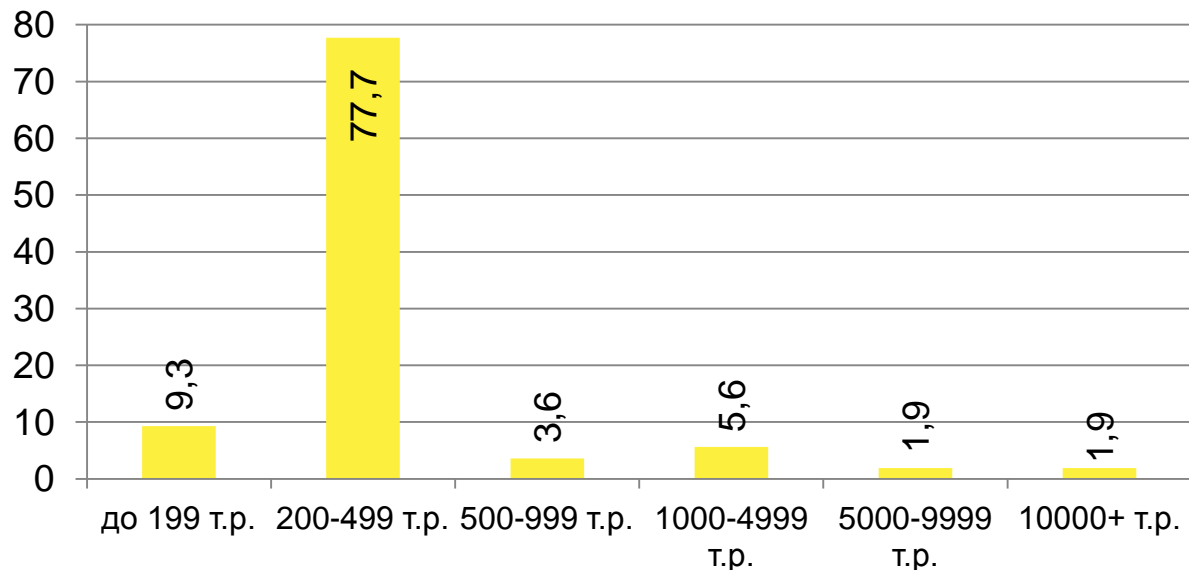


Электронное мошенничество. Результаты и тренды 2015

Распределение по суммам, %



Распределение по количеству транзакций, %



- 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

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/



Безопасность

[Подключение и восстановление доступа](#) [Платежи и переводы](#) [Возможности](#) [Тарифы и лимиты](#) **Безопасность**

[Вопросы и ответы](#) [Контакты службы поддержки](#)



Поиск



Банкоматы
и офисы



Интернет-
банк



Онлайн-
заявки



Контакты



Ваш город



Задумывались ли вы когда-нибудь, насколько вы готовы к встрече с настоящими интернет-мошенниками? Насколько надежными защитниками своих финансов являетесь вы сами?

С помощью короткого теста из 9 вопросов мы поможем оценить уровень готовности к противодействию попыткам мошенников получить доступ к вашим финансам.

А если результаты окажутся не самыми высокими, мы укажем на ошибки и расскажем, в чем суть того или иного вида мошенничества.

Готовы к тестированию? Тогда жмите на кнопку!

[Тест](#)

При входе в R-Connect всегда обращайте внимание, чтобы в правом нижнем углу или в адресной строке вашего браузера отображался значок защищенного соединения. Для проверки данных владельца сайта нужно дважды щелкнуть по значку, в данных «Сертификата безопасности» должен содержаться следующий текст:

CN = www.rconnect.ru

O = AO Raiffeisenbank

R Connect
Заходите, открыто!

[Подключить >](#)

РЕКОМЕНДУЕМ

[Мобильное приложение](#)

Ваш интернет-банк всегда под рукой. Просто скачайте приложение R-Mobile.

Скачать приложение можно в
App Store и **Google Play**:

Доступно в
App Store

доступно в
Google play

ЭТО МОЖЕТ БЫТЬ ПОЛЕЗНО

За 30 секунд [расскажем как подключить](#)
интернет-банк R-Connect.

СПАСИБО ЗА ВНИМАНИЕ !



ВОПРОСЫ?