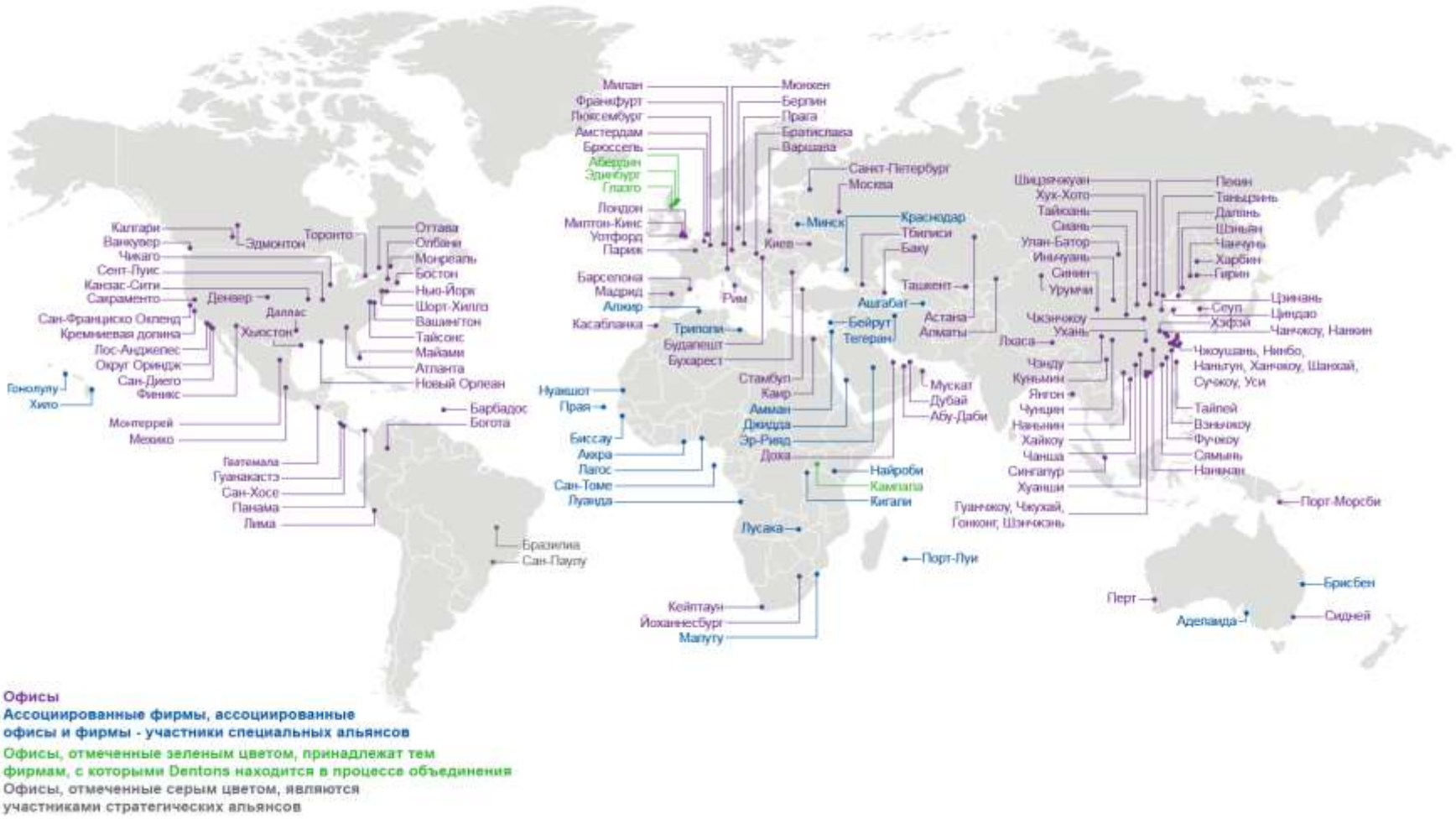
Актуальные угрозы информационной безопасности платежных систем и методы противодействия

Антон Поддубный
Советник

24 мая 2018 года

Dentons – самая крупная в мире юридическая фирма*



** 2017 The American Lawyer – Рейтинг 100 международных юридических фирм по количеству юристов (Global 100).*

Dentons в мире

Стран

66

Офисов

158

Количество юристов

8 600+

Количество сотрудников

15 000+

Кибератаки на различные отрасли в РФ

Согласно исследованиям международной консалтинговой компании PWC за 2017 г. **большинство российских компаний** не могут успешно противостоять кибератакам

Статистика Центрального Банка РФ за 2015-2017

* По данным официального отчета Центрального Банка РФ 2018
«Обзор несанкционированных переводов денежных средств за 2017 год»

БАНК РОССИИ
ФИНЦЕРТ

Статистика Центрального Банка РФ за 2015-2017

* По данным официального отчета Центрального Банка РФ 2018

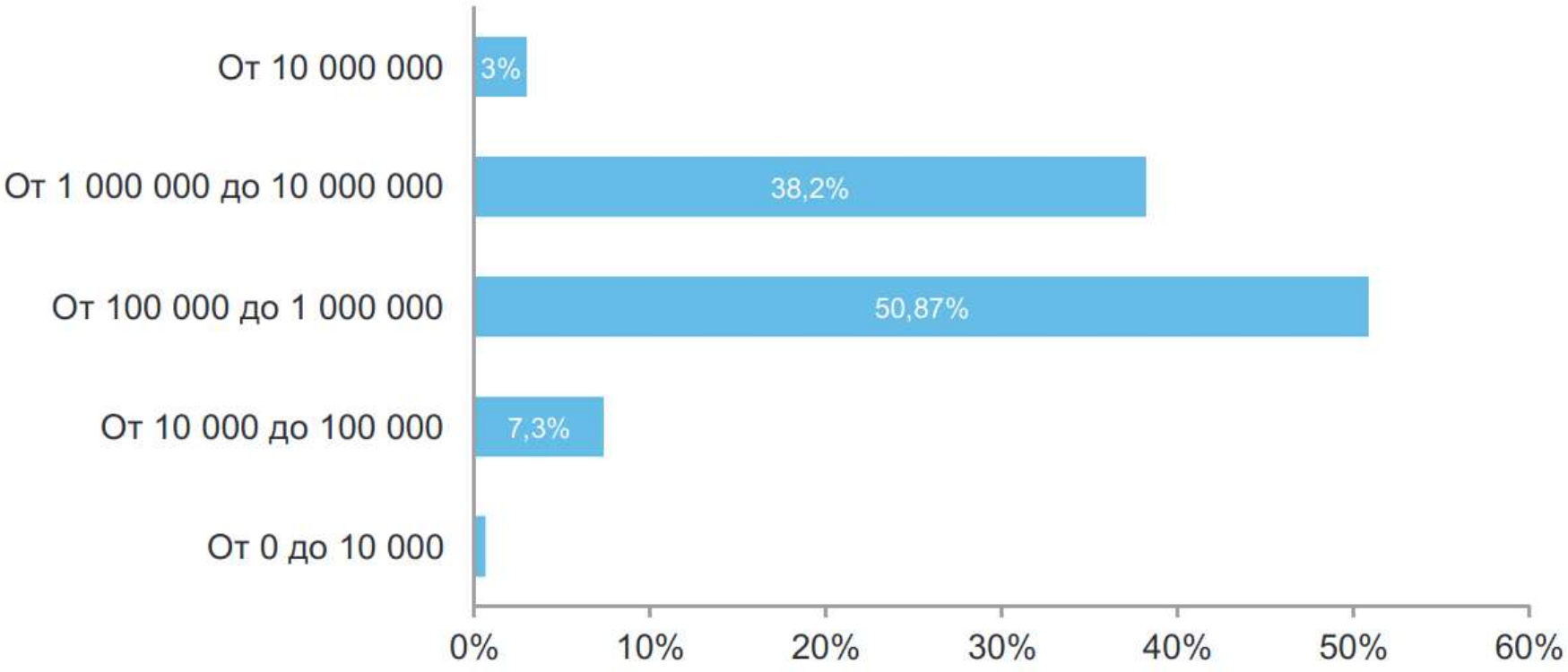
«Обзор несанкционированных переводов денежных средств за 2017 год»

БАНК РОССИИ ФИНЦЕРТ

Статистика Центрального Банка РФ за 2015-2017

* По данным официального отчета Центрального Банка РФ 2018

Распределение несанкционированных операций со счетов ЮЛ



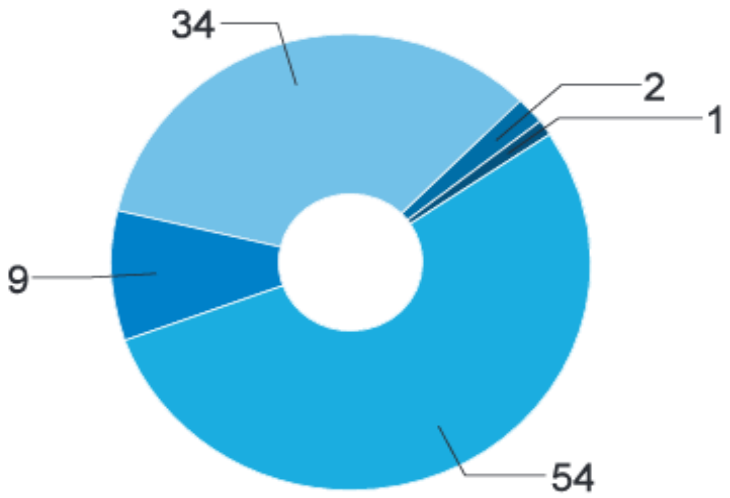
БАНК РОССИИ ФИНЦЕРТ

大成 DENTONS

Статистика Центрального Банка РФ за 2015-2017

* По данным официального отчета Центрального Банка РФ 2018

Распределение по причинам совершения несанкционированных операций со счетов ЮЛ



- Использование ЭСП без согласия клиента вследствие противоправных действий, потери, нарушения конфиденциальности (предположительно воздействие вредоносного кода)
- Нарушение клиентом порядка использования ЭСП
- Воздействие вредоносного кода
- Побуждение владельца ЭСП к совершению операции путем обмана или злоупотребления доверием
- Иная причина инцидента

БАНК РОССИИ ФИНЦЕРТ

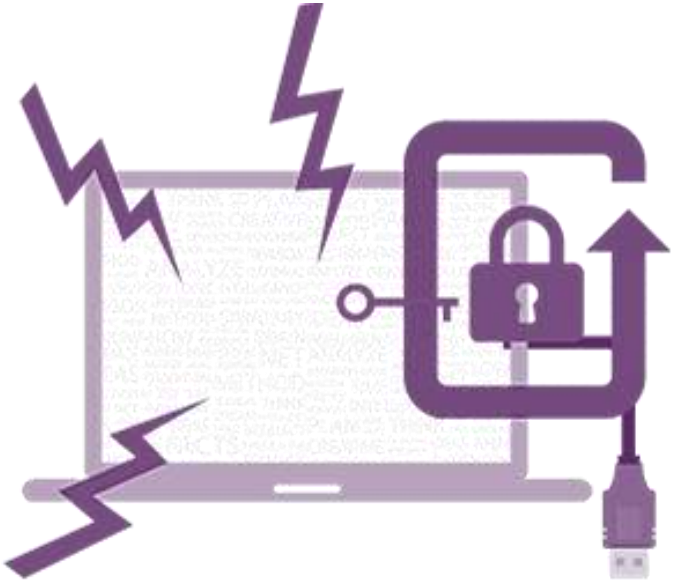
Правовое регулирование работы платежных систем

- **Федеральный закон N 161-ФЗ** «О Национальной платёжной системе»
  (закон гласит, что если клиент уведомляет банк о неправомерном использовании средств электронного платежа, банк обязан возместить ему сумму операции, совершённой без его согласия)
- **Федеральный закон N 63-ФЗ** «Об электронной подписи»
- **Положение Банка России № 382-П** «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»
- **Федеральный закон N 149-ФЗ** «Об информации, информационных технологиях и о защите информации»
- **ГОСТ Р 57580.1-2017** «Безопасность финансовых (банковских) операций, защита информации финансовых организаций базовый состав организационных и технических мер»
- **Федеральный закон от 26 июля 2017 г. N 187-ФЗ «**О безопасности критической информационной инфраструктуры Российской Федерации»
- **Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 29.07.2017)** «О персональных данных»
- **Комплекс БР ИББС**

Угрозы и атаки на платежные системы

ВНЕШНИЕ

- Хакеры
- Конкуренты
- Злоумышленники
- Преступные группы



ВНУТРЕННИЕ

- Персонал
- Инсайдеры
- Обслуживающие компании

Актуальные угрозы информационной безопасности
для клиентов платежных систем банка, систем ДБО

Вредоносное ПО (трояны, вирусы, кейлоггеры, клиенты бот-сетей и т.д.)	• Наиболее распространённый способ атаки, заражения вирусами, троянами персонального компьютера клиента для получения информации и управления
Социальная инженерия	• Набирающий популярность метод получения необходимого доступа к информации, основанный на особенностях психологии людей, с применением технических средств
Внутренние атаки инсайдеров, персонала	• Собственные нелояльные сотрудники организации, пытающиеся получить конфиденциальные сведения или личную выгоду, шантаж работодателя
Использование атак типа Man-in-the-Middle для проведения подложных транзакций	• Вид атаки, когда злоумышленник тайно ретранслирует и, возможно, изменяет связь между двумя сторонами прошедших аутентификацию
Использование уязвимостей ПО	• Реализация заведомо известных уязвимостей в программном коде для получения контроля и данных системы

Основные угрозы информационной безопасности
для клиентов платежных систем банка, систем ДБО

Вредоносное ПО (трояны, вирусы, кейлогеры, клиенты бот-сетей и т.д.)

К категории «банковских троянов» относятся:

- **Вредоносные программы**, предназначенные для похищения конфиденциальной информации и обеспечения несанкционированного доступа к системам дистанционного банковского обслуживания (ДБО). Многие банковские трояны сочетают в себе функции **бэкдора** и **шпионских программ**

- Наиболее распространенным методом проникновения банковских троянов в операционную систему является **их загрузка другими вредоносными программами – троянами-загрузчиками**

- Также большую опасность представляет возможность заражения **при просмотре инфицированных веб-страниц** — с использованием различных уязвимостей прикладного ПО

- Помимо этого, банковские трояны могут проникнуть на компьютер жертвы **в виде вложений в сообщения**, массово рассылаемые по каналам электронной почты, **на инфицированных съемных носителях, с использованием методов социальной инженерии**

Основные угрозы информационной безопасности
для клиентов платежных систем банка, систем ДБО

Социальная инженерия

Метод получения необходимого доступа к информации, основанный на особенностях психологии людей. Основной целью социальной инженерии является **получение доступа к конфиденциальной информации, паролям, банковским данным и другим защищенным системам**

ПРЕТЕКСТИНГ - набор действий, отработанных по определенному сценарию, в результате которого жертва может выдать информацию или совершить действие. Чаще всего предполагает использование голосовых средств, таких как Skype, телефон и т.п.

ТРОЯНСКИЙ КОНЬ основывается на любопытстве или страхе пользователей. Злоумышленник отправляет электронное письмо жертве, во вложении которого находится «обновление» антивируса, ключ к денежному выигрышу или компромат на сотрудника.

ДОРОЖНОЕ ЯБЛОКО - использование носителей (CD, флэш-накопителей). Злоумышленник подбрасывает «зараженный» носитель в общедоступных местах на территории компании.

ФИШИНГ направлен на получение конфиденциальной информации. Фишинговой атакой является поддельное письмо по электронной почте, которое выглядит как официальное письмо от платежной системы или банка. В письме содержится форма для ввода персональных данных (пин-кода, логина и пароля) или ссылка на web-страницу, где располагается такая форма.

КВИ ПРО КВО (услуга за услугу) предполагает обращение по эл. почте или телефону. Злоумышленник может представиться сотрудником техподдержки и сообщить о необходимости устранения технических проблем на рабочем месте. В процессе «решения» такой проблемы злоумышленник подталкивает жертву на совершение действий, позволяющих атакующему установить необходимое программное обеспечение на компьютере.

ОБРАТНАЯ СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ побуждает жертву обратится к злоумышленнику за «помощью». Например, злоумышленник может выслать письмо с контактами «службы поддержки» и создать обратимые неполадки в компьютере жертвы. В процессе «исправления» проблемы злоумышленник сможет получить необходимые ему данные

Основные угрозы информационной безопасности
для клиентов платежных систем банка, систем ДБО

Внутренние атаки инсайдеров, персонала

Как правило, нелояльные сотрудники являются достаточно распространённой угрозой платёжным системам банка

Неблагонадёжные родственные связи, обида на начальство, неоцененность, корыстные цели, сложные жизненные обстоятельства – основные причины, которые побуждают персонал организации клиента идти на мошенничество, связанное с платежными системами

Самая опасная и легко реализуемая угроза – когда персонал имеет доступ к авторизационным данным и ключевым носителям для работы с платёжной системой.

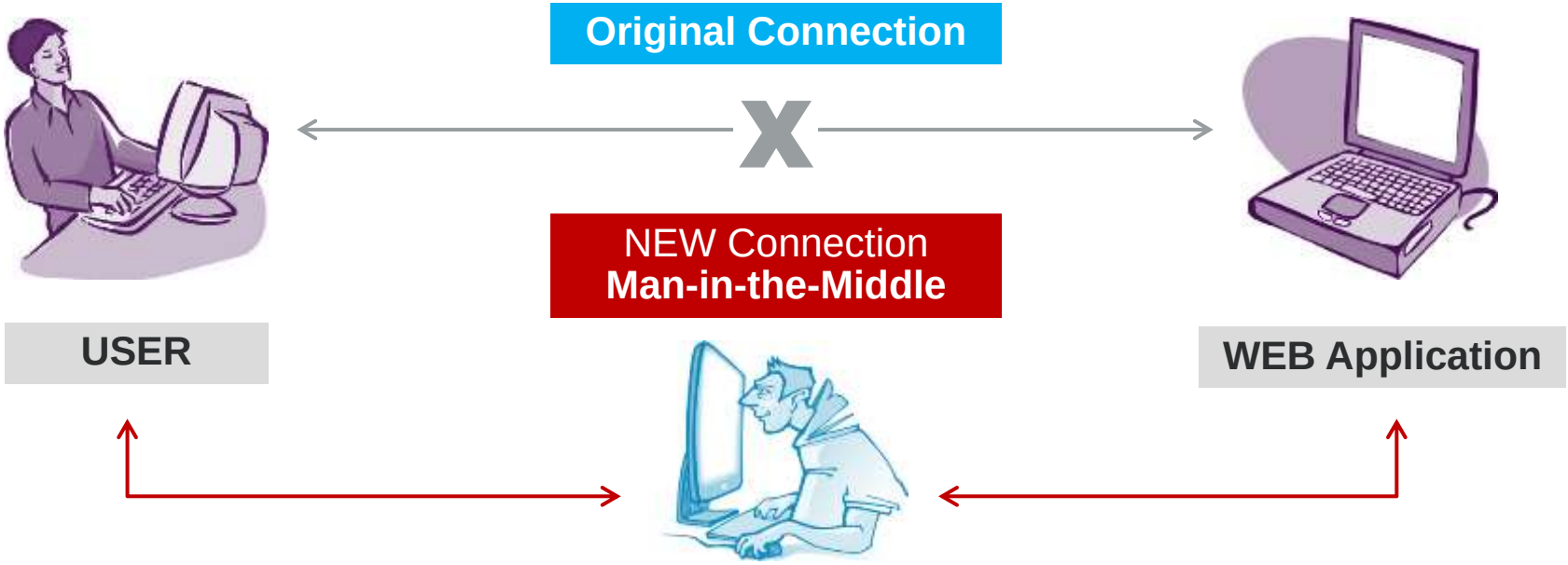
Доступ к данным может повлечь мошенничества, кражи конфиденциальной и коммерчески ценной информации, воровство интеллектуальной собственности, саботаж компьютерных систем.

Основные угрозы информационной безопасности
для клиентов платежных систем банка, систем ДБО

Атаки типа Man-in-the-Middle для проведения подложных транзакций

Внедрение кода для захвата уже авторизованной сессии, **выполнения собственных команд на сервере и отправки ложных ответов клиенту.** Метод позволяет злоумышленнику вставлять свой код в электронные письма, SQL-выражения и веб-страницы, а также модифицировать загружаемые пользователем файлы в целях получения доступа к учетной записи пользователя.

Клиент на экране может видеть легитимный платеж, в то время как на сервер банка уходит платёж с изменёнными реквизитами



Основные угрозы информационной безопасности
для клиентов платежных систем банка, систем ДБО

Использование уязвимостей ПО

Платежные системы представляют собой **приложения, состоящие из программного кода.**

Для них характерны все уязвимости, известные в сфере безопасности приложений, а также угрозы, связанные со спецификой банковской сферы: ***хищение денежных средств, несанкционированный доступ к данным, к банковской тайне, отказ в обслуживании и другие угрозы, реализация которых может привести к существенным финансовым и репутационным потерям***

- Наиболее часто встречаются уязвимости, позволяющие получить **несанкционированный доступ к данным пользователей.** К этой категории в основном относятся недостатки авторизации.

- Уязвимости приложений также связаны с «Недостаточной защитой сессии» (некорректное завершение сессий пользователей, некорректная настройка параметров, возможность параллельной работы с несколькими сессиями для одного пользователя, отсутствие привязки сессии к IP-адресу клиента).

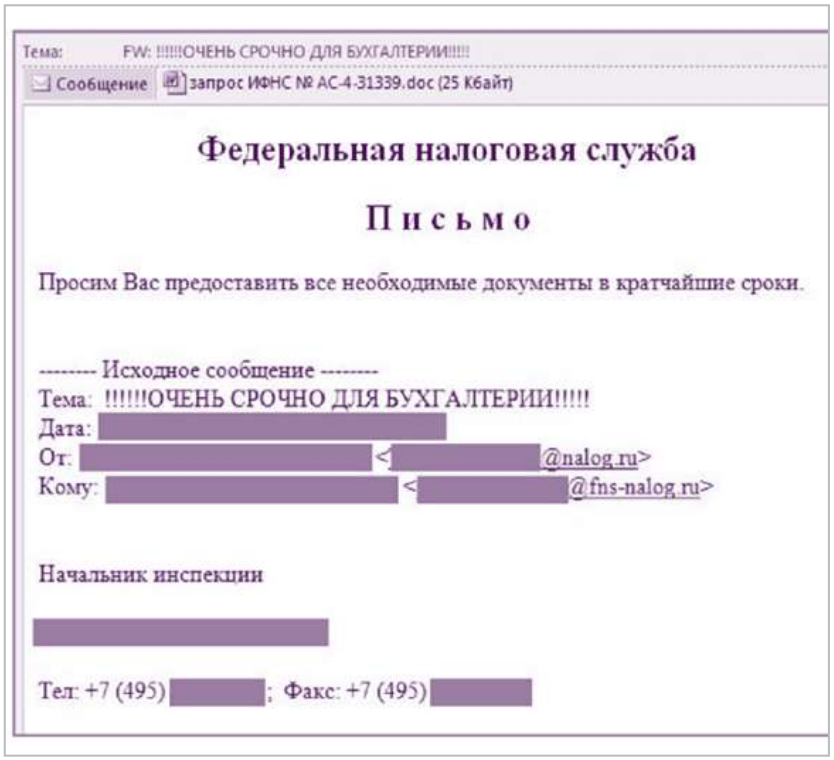
Основные причины возможности реализации угроз
на стороне клиентов платежных систем банка, систем ДБО

1. Отсутствие полноценных служб **«Информационной Безопасности»** и **«Отделов информационных систем»**
2. Не обеспечена должным образом **сетевая защита в компании**, не настроены межсетевые экраны; отсутствие **противовирусных программных средств**
3. Отсутствие **разграничения прав пользователя** на используемом персональном компьютере
4. Не проводятся **своевременные обновления операционной системы** и программных продуктов
5. **Бесконтрольный доступ** к персональному носителю ключевой информации, нарушение правил хранения
6. Использование персонального компьютера для **бесконтрольного «серфинга»** в сети интернет
7. Очень **слабая осведомлённость персонала** в вопросах информационной безопасности
8. Передача аутентификационной информации и ключевых носителей **третьим лицам**

Примеры реализации угроз и атак

* По данным расследований реальных случаев хищений средств («Лаборатория Касперского»)

Распространенный вид смешанных атак


Тема: FW: !!!!!ОЧЕНЬ СРОЧНО ДЛЯ БУХГАЛТЕРИИ!!!!!

Сообщение | запрос ИФНС № АС-4-31339.doc (25 Кбайт)

Федеральная налоговая служба

П и с ь м о

Просим Вас предоставить все необходимые документы в кратчайшие сроки.

-------- Исходное сообщение --------
Тема: !!!!!ОЧЕНЬ СРОЧНО ДЛЯ БУХГАЛТЕРИИ!!!!!
Дата: [redacted]
От: [redacted] <[redacted]@nalog.ru>
Кому: [redacted] <[redacted]@fns-nalog.ru>

Начальник инспекции

[redacted]

Тел: +7 (495) [redacted]; Факс: +7 (495) [redacted]

1. В ходе целевой атаки с использованием социальной инженерии и уязвимости в программе Microsoft Word компьютер бухгалтера был заражен **Backdoor.Win32.RMS**

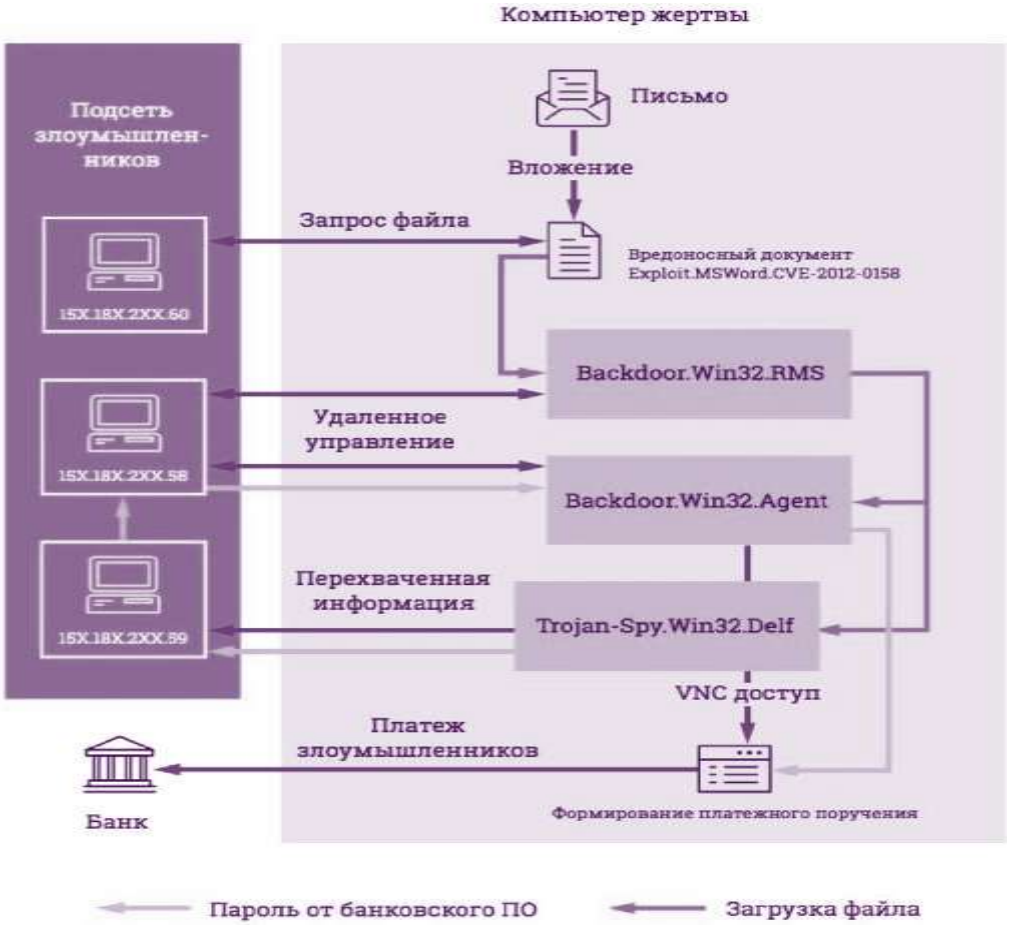
2. С помощью этого бэкдора злоумышленники загрузили на зараженную машину еще две вредоносные программы: **кейлоггер** (Trojan-Spy.Win32.Delf) и **бэкдор** (Backdoor.Win32.Agent), предоставляющий удаленный VNC доступ к компьютеру жертвы

3. Кейлоггер перехватил пароль для доступа к системе ДБО

Примеры реализации угроз и атак

* По данным расследований реальных случаев хищений средств («Лаборатория Касперского»)

Распространенный вид смешанных атак



4 Пока бухгалтера не было на рабочем месте, злоумышленники с помощью **Backdoor.Win32.Agent**, используя VNC доступ к компьютеру, запустили от имени бухгалтера банковское ПО

5 Использовав пароль, перехваченный кейлоггером, киберпреступники сформировали и отправили в банк **платежное поручение на сумму около 300 тыс. руб.**

6 Чуть позже было сформировано и отправлено в банк еще одно платежное поручение – приблизительно на **3 млн. руб.**

Риски

ФИНАНСОВЫЕ

- Потери и приостановление операционной деятельности

ПРАВОВЫЕ

- Иски клиентов и контрагентов
- Компрометирование конфиденциальной информации
- Уголовная ответственность (п. 3 ст. 274.1 УК РФ)
- Отсутствие прямой административной ответственности (13.11 КоАП), но возможность стать объектом пристального внимания Роскомнадзора и получения предписания от Роскомнадзора, включая проверку с участием ФСТЭК

Методы противодействия

1. ТЕХНИЧЕСКИЕ
2. РАБОТА С ПЕРСОНАЛОМ
3. ПОСТРОЕНИЕ СТРУКТУРЫ МОНИТОРИНГА И КОМПЛАЕНСА
4. КОНТРАКТНАЯ РАБОТА
5. СТРАХОВАНИЕ ОТВЕТСТВЕННОСТИ

Методы противодействия

1 ТЕХНИЧЕСКИЕ

Современные технические решения

- двух-уровневая идентификация / биометрическая идентификация
- запрет на использование съемных носителей информации
- обновление ПО

Удачные проекты, связанные с биометрической идентификацией

- Сбербанк использует лицевую биометрию в кредитном процессе уже около пяти лет.
- В мобильных приложениях "ВТБ-Онлайн" для клиентов может быть настроен вход по отпечатку пальца.
- Почта Банк начал использовать биометрическую верификацию клиентов с 2014 года, а сотрудников — с 2017-го.
- В 2014 году Тинькофф Банк начал использовать технологии распознавания клиентов по голосу.
- По словам главного системного архитектора Альфа-Банка Сергея Радула, как только появились первые iPhone с функцией Touch ID, Альфа-Банк одним из первых сделал вход в мобильное приложение "Альфа-Мобайл" с использованием этой функции.

Методы противодействия

2 **РАБОТА С ПЕРСОНАЛОМ**

Тренинги по кибербезопасности и безопасному поведении в сети

Методы противодействия

3

ПОСТРОЕНИЕ СТРУКТУРЫ МОНИТОРИНГА И КОМПЛАЕНСА, РАСКРЫТИЕ ИНФОРМАЦИИ

Наблюдение, разработка и внедрение политик и должностных инструкций

Методы противодействия

4 **КОНТРАКТНАЯ РАБОТА**

Ответственность поставщиков оборудования и ПО

+

исключение ответственности
в случае противоправных действий третьих лиц

Методы противодействия

5

СТРАХОВАНИЕ ОТВЕТСТВЕННОСТИ

Методы противодействия

В ЧЕМ СИЛА, БРАТ?

** в комплексном решении*

Контакты

Антон Поддубный

Советник

T +7 812 325 84 44

M +7 921 960 83 36

anton.poddubny@dentons.com

Спасибо за внимание!

大成 DENTONS

Dentons в Санкт- Петербурге

БЦ «Дженсен Хауз»

Невский пр., д. 32- 34, лит. А

191011, **Санкт- Петербург**

Российская Федерация

Вид с террасы офиса Dentons в Санкт- Петербурге

Dentons – крупнейшая в мире юридическая фирма*, предоставляющая полный спектр юридических услуг. Dentons входит в число лидеров рейтинга ведущих юридических брендов мира, составленный Acritas, получила награду BTI Client Service 30 Award, а также – высокую оценку деловых и юридических изданий за инновации, включая создание Nextlaw Labs и Nextlaw Global Referral NetworkDentons предоставляет юридические услуги российским и иностранным компаниям, банкам и другим финансовым институтам, фондам прямых инвестиций, государственным предприятиям и некоммерческим организациям. www.dentons.com

** 2017 The American Lawyer – Рейтинг 100 международных юридических фирм по количеству юристов (Global 100).*