Кража со взломом. Как защитить банковскую карту от мошенников нового типа

Елена Изюмова Forbes Contributor

Фото Donal Husni / Zuma / TASS

Банковские операции в интернете по-прежнему небезопасны: хакеры придумывают новые способы вывода денег со счетов. Чаще всего жертвами становятся клиенты-физлица. Как обезопасить свои счета от атак?

За последние два года ущерб от кибератак в банковской сфере в России составил более 8 млрд рублей. При этом около половины денег было украдено не у самих кредитных организаций, а напрямую у их клиентов – физических и юридических лиц. Об этом говорится в ежегодном отчете IT-компании Group-IB о преступлениях в сфере высоких технологий, который был опубликован 10 октября.

По данным исследования, каждый клиентский сегмент страдает от действий хакеров в разной степени. За два года у юридических лиц, использующих интернет-банкинг, украли 1,6 млрд рублей. Чуть меньше хакеры похитили у физлиц. С помощью вредоносных программ для Android они «собрали» 1,2 млрд рублей, с использованием троянов для ПК – 22 млн рублей.

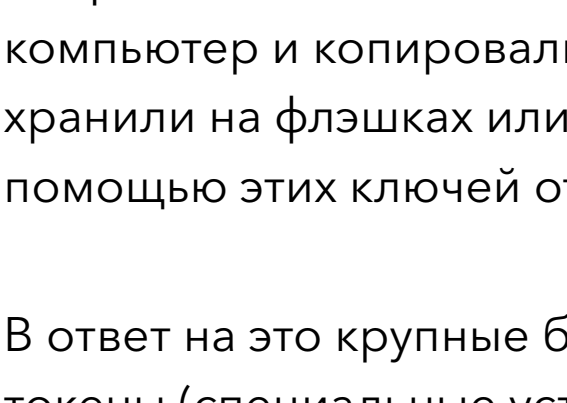
При этом именно в сегменте физических лиц за последний год (с апреля 2016 по апрель 2017 года) отмечен наибольший рост ущерба – он составил 136% у владельцев гаджетов на Android (до 821 млн рублей) и 144% – у жертв троянов для ПК (до 15,7 млн рублей). Для сравнения: объем похищенных средств у корпоративных клиентов, напротив, сократился за этот же период на 35% до 622 млн рублей.

Охота на «корпората»

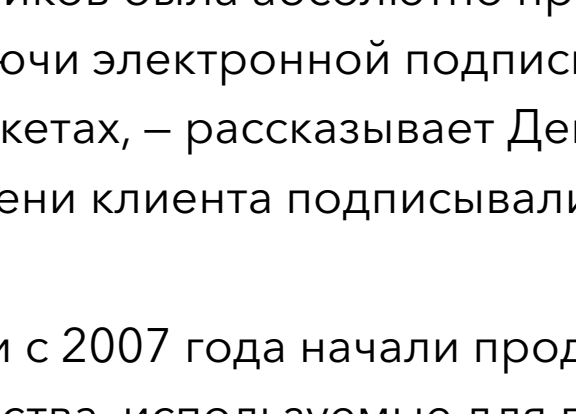
Опрошенные эксперты отмечают, что традиционно мишенью для хакеров выступали прежде всего корпоративные клиенты банков. Кражи на крупные суммы, которые могут составлять от нескольких сот тысяч до десятков миллионов рублей, интереснее злоумышленникам и в большей степени оправдывают риски, связанные с незаконной деятельностью, объясняет региональный представитель компании «Уральский центр систем безопасности» Алексей Комаров.

Генеральный директор компании SafeTech Денис Калемберг добавляет, что в 87% случаев у юридических лиц крадут суммы в пределах от 100 000 рублей до 10 млн рублей за раз, но случаются кражи и масштабнее. Так, в 2016 году у одной крупной логистической компании похитили сразу 236 млн рублей, приводит пример эксперт.

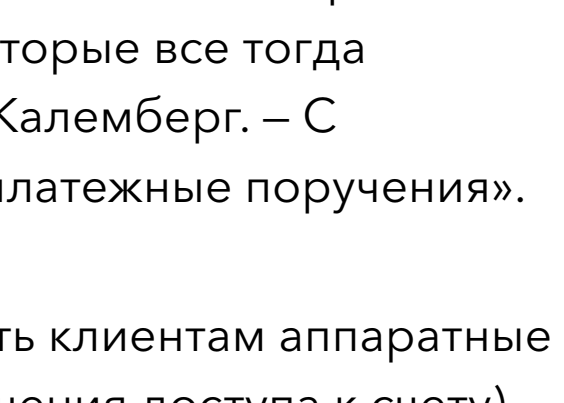
МАТЕРИАЛЫ ПО ТЕМЕ



Опасная транзакция: пять актуальных киберугроз для банков и их клиентов



Проверка на прочность: зачем создатели вируса BadRabbit атаковали СМИ и банки



Опасный Wi-Fi. Как защитить компьютеры и телефоны от взлома

По его словам, активно похищать деньги у юрлиц через дистанционное банковское обслуживание (ДБО) хакеры начали еще в 2006 году, и с тех пор технологии стали более продвинутыми.

«Первая технология мошенников была абсолютно примитивной: они заражали компьютер и копировали ключи электронной подписи, которые все тогда хранили на флэшках или дискетах, – рассказывает Денис Калемберг. – С помощью этих ключей от имени клиента подписывались платежные поручения».

В ответ на это крупные банки с 2007 года начали продавать клиентам аппаратные токены (специальные устройства, используемые для получения доступа к счету) – с них украсть ключ подписи было намного сложнее. В результате рост убытков у клиентов замедлился, но только на время, вспоминает эксперт.

В 2009 году появились токены «с неизвлекаемым ключом», и специалисты по информационной безопасности банков оптимистично назвали их «панацеей от краж в ДБО».

Однако уже в 2010 году хакеры сменили тактику и начали воровать деньги с использованием удаленного подключения к компьютеру бухгалтера – от этого токены уже не спасали. Поэтому банковским клиентам предлагалось на каждую операцию вводить дополнительный одноразовый пароль (он генерировался в отдельном устройстве или приходил по SMS).

«Это было очень неудобно, и помогало недолго, так как в 2011 году появилась самая совершенная технология атаки – «автоматическая подмена реквизитов», или «автозалив», – уточняет Денис Калемберг.

Технология работает так: когда компьютер клиента заражается, троян автоматически меняет данные платежа, которые уходят на подпись в токен. При этом пользователь видит на экране своего компьютера платежку, вводит все необходимые коды и даже не подозревает, что перечисляет деньги мошенникам.

Генеральный директор компании Group-IB Илья Сачков добавляет, что при совершении атак на юридических лиц злоумышленники могут подменять реквизиты 1С или использовать удаленное управление, чтобы совершать необходимые транзакции в ручном режиме

Финансы под угрозой

Сокращение объема краж в корпоративном сегменте за последний год Сачков связывает с тем, что хакеры стали тщательнее выбирать жертв (средняя сумма одной кражи выросла до 1,25 млн рублей). Кроме того, резко сократилось число преступных групп, занимающихся работой с юрлицами, а банки начали активно внедрять системы класса антифрод, которые блокируют подозрительные операции по выводу средств со счета.

Таким образом, опрошенные эксперты сходятся во мнении, что усилия хакеров теперь сконцентрированы на частных пользователях, управляющих своими счетами с домашнего компьютера или смартфона.

Согласно данным Group-IB, больше всего клиенты-физлица пострадали от атак на смартфоны на базе Android. Эксперты компании объясняют это тем, что почти 85% смартфонов в мире работают на этой платформе. В отличие от iOS, это открытая экосистема с незначительной цензурой, поэтому неудивительно, что большинство вирусов пишутся именно под нее, подчеркивается в исследовании Group-IB.

Денис Калемберг считает, что основной причиной роста успешных атак на счета физлиц является технологическая легкость кражи паролей и кодов подтверждения операций.

«Практически все банки отправляют их через SMS, а этот канал изначально не был предназначен для передачи конфиденциальной информации», – разъясняет эксперт.

Злоумышленникам не составляет особого труда перехватить такое SMS-сообщение техническим способом – например, заразив смартфон клиента «трояном», либо перевыпустив SIM-карту по поддельной доверенности, добавляет Калемберг.

Впрочем, по мнению Ильи Сачкова, именно ориентация новых групп хакеров на получение данных банковских карт, а не на перехват SMS, позволила повысить средний ущерб от одной атаки.

К примеру, злоумышленники заражают устройство на Android и получают из него данные банковской карты либо логин/пароль от интернет-банка, а также информацию о текущем балансе. Если баланс пользователя вызовет интерес, то мошенники привязывают на своем iPhone банковский счет жертвы к Apple Pay.

Для этого они используют полученные данные карты или логин/пароль, а также смс-подтверждения, которые успешно перехватывает Android-троян. После этого они могут совершать покупки, не имея физической карты. Впрочем, мошенники вынуждены отовариваться в определенных точках – если суммы большие, платежный терминал может запросить ПИН-код. К тому же только у части банков есть список доверенных точек, в которых ПИН-код никогда не требуется.

Можно ли вернуть деньги

Все опрошенные специалисты отметили, что если злоумышленники успели вывести деньги со счета, а внутренние системы банка пропустили платеж, то отменить его уже невозможно.

Теоретически можно оспорить транзакцию, или попытаться заблокировать деньги на счете получателя на основании N 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», но, скорее всего, уже через несколько часов деньги будут обналичены в банкоматах.

В этой ситуации остается лишь одна опция – доказать, что банк не сделал все возможное для обеспечения безопасных платежей, и получить с него возмещение убытков, считает эксперт компании RTM Group Евгений Царев. Он советует сразу же обращаться в правоохранительные органы и требовать возбуждения уголовного дела.

Кроме того, необходимо привлечь эксперта по информационной безопасности. Его основной задачей будет сбор доказательств невыполнения банком существующих требований по защите информации и бездействия по предотвращению инцидента. Также необходимо убедить суд, что сам клиент выполнил все требования по информационной безопасности, а также проявил должную осмотрительность.

«Если в 2016 году практически не было дел, где была бы доказана прямая вина банка в хищении через ДБО, то судебная практика по делам 2017 года дает возможность надеяться на полное или частичное возмещение убытков. Кроме того, заключен ряд мировых соглашений, которые также подразумевают выплату компенсаций», – комментирует Евгений Царев.

Небольшому или региональному банку крайне сложно выполнить весь спектр отраслевых и законодательных требований по защите информации, поэтому нарушения в любом случае будут. Также следствие обычно запрашивает экспертизу безопасности самописных систем, например, ДБО, где тоже можно выявить нарушения, добавляет эксперт.

Как защититься

Для противодействия мошенникам специалисты советуют не полагаться на один способ защиты, а использовать комбинацию технических и организационных мер.

Корпоративная защита

Чаще всего бухгалтерский ПК находится в общей корпоративной сети. Поэтому меры защиты должны быть обеспечены в масштабе всей организации;

- В дополнение к антивирусной защите (ее необходимость не обсуждается), необходимо применять дополнительные средства безопасности сети: межсетевые экраны, обнаружение вторжений, антиспам, системы класса «песочница»;
- Необходимо следить за своевременной установкой обновлений всех операционных систем и приложений;
- Надо постоянно проводить обучение пользователей принципам «цифровой гигиены»: не переходить по подозрительным ссылкам, не открывать почтовые вложения от непроверенных адресатов, не использовать неизвестные носители информации, тщательно хранить пароли;
- При проведении платежей можно использовать так называемые «трастскрины», аппаратные устройства с «доверенной средой», которые отображают настоящие реквизиты платежа и блокируют его подписание до тех пор, пока клиент не подтвердит операцию нажатием кнопки на корпусе устройства;
- Внимательно изучите договор с банком на предоставление услуг ДБО. Если там прописано применение определенных мер защиты – использовать их надо обязательно.

Защита личного ПК

Если вы проводите операции с личными финансами через свой персональный компьютер или ноутбук, то необходимо соблюдать следующие принципы:

- Обязательно используйте не просто антивирусную программу, а продукт класса Internet Security, который содержит встроенный файервол. Обычно это платные продукты, даже если базовая версия антивируса бесплатна.
- Скачивайте и сразу устанавливайте все обновления операционной системы и приложений;
- Никогда не используйте публичную сеть wi-fi для доступа к интернет-банку;
- Не переходите по подозрительным ссылкам, не открывайте почтовые вложения от непроверенных адресатов, не используйте неизвестные носители информации, тщательно храните и периодически меняйте пароли.

Защита смартфона

Злоумышленники очень активно разрабатывают новые технологии троянов для Android, поэтому использовать интернет-банкинг на смартфоне нужно крайне осторожно:

- установите антивирусное приложение;
- используйте для общения с банком, приема или передачи подтверждающих смс-сообщений другой телефон, лучше всего, не смартфон;
- никогда не используйте публичную сеть wi-fi для доступа к интернет-банку;
- не переходите по подозрительным ссылкам, не открывайте почтовые вложения от непроверенных адресатов, не устанавливайте малоизвестные приложения;
- используйте программу класса «подпись в смартфоне» или программный «тасткрин в смартфоне».

банки банковские карты кибербезопасность