Современная система антифрода: выявлять и защищать!

Андрей Луцкович, директор ООО "Фродекс"

Деньги клиентов банков всегда были и остаются лакомым кусочком для нечистых на руку элементов. Как оказалось, повсеместный переход на дистанционное банковское обслуживание упростил жизнь не только банкам и их клиентам, но и мошенникам. С одной стороны, исчезла необходимость в посещении банка, а с другой – у мошенников появились новые возможности доступа к кошельку клиента. Поэтому сегодня уже каждый банк имеет собственную статистику инцидентов, и от рассуждений о необходимости систем антифрода переходит к их выбору и внедрению.

Традиционно мошенничество в дистанционном банковском обслуживании, как, впрочем, и любое другое, основано на искажении информации, которой обмениваются стороны сделки. При очном посещении банка клиент точно знает, куда он пришел и с кем общается. Банк, в свою очередь, удостоверяется в личности пришедшего. Конечно, находятся умельцы, успешно проворачивающие темные делишки и в этих условиях, но это сложно и требует либо халатности, либо коррумпированнности ответственного банковского сотрудника.

Информационные технологии позволили территориально разнести клиента и сотрудника банка, но потребовали изобретать новые способы идентификации клиента и обеспечения безопасности. Нельзя сказать, что банковское сообщество не предприняло усилий, клиентам предоставили некоторые средства защиты для работы в информационных системах: пароли, криптографические ключи. Но статистика инцидентов показала, что этого недостаточно.

Изначально, столкнувшись с разрастанием использования дистанционного банковского обслуживания для мошенничества, банки пошли по пути перенесения вины на клиентов. Банки посчитали, что оснастили клиента всем необходимым, а клиент виноват в том, что предоставил мошенникам доступ к информации, необходимой для авторизации, не соблюдая требования информационной безопасности.

Но давайте разберемся, в чем, на самом деле, обвиняется клиент. По сути, только в том, что не обеспечил чистоту собственного устройства (персонального компьютера, планшета, смартфона) от вирусного программного обеспечения мошенников. Специализированные банковские вирусы позволяют украсть все необходимое для доступа в банковскую систему и подтверждения транзакций, что позволяет действовать от имени клиента или, что еще хуже, выполнить мошеннические платежи непосредственно с устройства клиента. Добавим сюда максимальную скрытность подобного программного обеспечения. В итоге клиент обнаруживает недостаток средств на счетах и транзакцию, которую он не выполнял. Банк же справедливо возражает и указывает на использование в этой транзакции всех необходимых атрибутов подтверждения клиента.

В большинстве случаев клиенты действительно пренебрегают разумными требованиями информационной безопасности, например, держат постоянно подключенными к ПК ключевые носители или же не оснащают свои устройства антивирусными средствами. Но необходимо признать, что выполнение требований не дает гарантии отсутствия инцидентов. Свидетельство тому – наличие фактов мошенничества с устройств, оснащенных средствами антивирусной защиты. К сожалению, всегда есть задержка между появлением новой версии банковского вируса и обновлением антивирусных баз. Индустрия кибермошенничества прилагает максимум усилий, чтобы это время было достаточным для совершения атаки на счета клиента банка.


Андрей Луцкович

Как следствие, у банка отсутствует доверие к информации, поступающей от клиента.

Система антифрода FraudWall

Вполне логичным шагом повышению доверия к информации от клиента стал ее предварительный анализ на стороне банка. Пришли к выводу: раз защитить нельзя, то будем выявлять подлоги. Выявление аномалий в клиентском потоке информации позволило банкам выбирать подозрительные операции и принимать решение по транзакции после обратной связи с клиентом. Началось широкомасштабное использование так называемых антифрод-систем (от анг. Fraud- мошенничество). Более трех лет тому назад наличие компетенций сотрудников компании Фродекс позволило предложить рынку собственную разработку – систему FraudWall.

Первоначально внедрение системы антифрода давало прорывной эффект

в борьбе с мошенничеством: обнаруживались практически все платежи, созданные не на устройстве клиента. Однако мошенники адаптировались, и со временем всё больше платежей стало приходить непосредственно с устройств клиентов. Практически возможны только два способа выполнить подобное: либо произвести удаленное подключение к устройству клиента и выполнить платеж, либо произвести так называемую автозамену реквизитов платежа, создаваемого непосредственно клиентом. И то, и другое проходит не без помощи вирусного программного обеспечения.

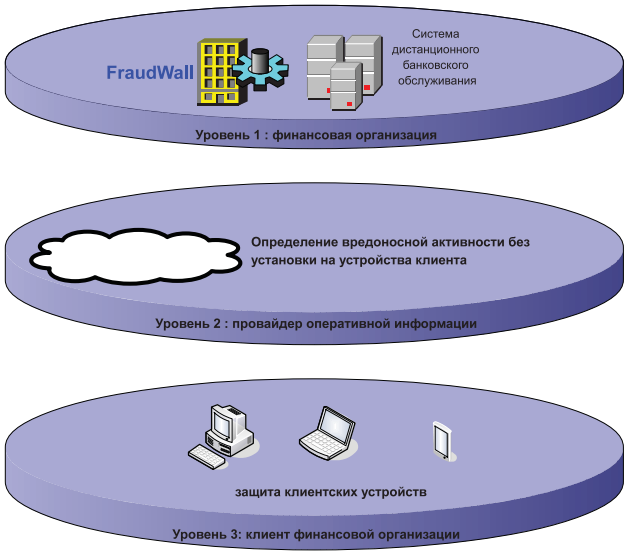
Задача по выявлению подобных мошеннических платежей потребовала реализовать в системе FraudWall более глубокий и полный анализ всей поступающей информации от клиента на сторону банка. Полученные результаты позволили обеспечить достаточный уровень обнаружения, и были по достоинству оценены банками клиентами компании Фродекс.

Но есть некоторые оговорки. Работа любой системы антифрода характеризуется двумя главными параметрами: количество пропущенных мошеннических платежей и количество ложных срабатываний. Это всегда взаимосвязанные величины. Чем больше наше желание не пропустить мошеннический платеж, тем большее число платежей система сочтет подозрительными и отправит на проверку через обратную связь с клиентом. Качество работы системы FraudWall проявляется в балансе между отбраковкой мошеннических платежей и приемлемом, с точки зрения трудозатрат банка, количестве платежей для проверки.

Однако, необходимо признать, что эти результаты были достигнуты для клиентов – юридических лиц. Банки изначально были больше озабочены именно юрлицами, как, впрочем, и мошенники. Денег на счетах юридических лиц гораздо больше, и размер средней транзакции, соответственно, тоже. Юридические лица более стабильны в собственной деятельности, поэтому более прогнозируемы, что дает положительные результаты при применении статистических методов обработки информации.

А вот транзакции физических лиц остаются головной болью для банков. Поведение физических лиц менее предсказуемо, средняя сумма транзакции меньше. Ущерб по конкретному инциденту может быть и невелик, но с точки зрения клиентской базы их обычно гораздо больше. Да еще законодательство в лице ФЗ-161 «О национальной платежной системе» требует вернуть деньги физическому лицу или доказать виновность клиента. Мошенники тоже понимают сложность выявления платежей на более мелкие суммы: снижается средняя сумма мошенничества, но взамен они стараются автоматизировать процессы и охватить максимальное количество потенциальных жертв.

[Рисунок 1] Сервис FraudTrack



Все это заставляет искать новые решения проблемы, в том числе и для клиентов – физических лиц.

Антифрод-сервис FraudTrack

Одним из ключевых факторов бурного развития кибермошенничества в последние годы является широкомасштабное объединение усилий преступников. Характерной чертой этой индустрии становится постоянный обмен информацией о разработанных технологиях. Это проявляется в периодическом появлении в общем доступе исходных кодов специализированного вредоносного программного обеспечения. Что, несомненно, дает толчок к дальнейшему развитию мошеннических технологий.

Еще одна черта современной киберпреступности – переход на использование бизнес-модели SaaS (software as a service — программное обеспечение, как услуга). Предоставление программных средств для совершения киберпреступлений в аренду позволяет одним обеспечить себе стабильный заработок, другим – снижает стоимость входного билета на рынок мошенничества и требования к знаниям и навыкам в области информационных технологий. Это дало толчок к приходу в эту область представителей традиционного криминального мира.

Что же наблюдается на другой стороне баррикад? Неэффективность большинства используемых мер показывает необходимость модернизации парадигмы защиты. Речь идет именно об эффективности: еще недавно прежних мер было достаточно, сейчас уже нет. Рост клиентской базы сопровождается пропорциональным ростом количества попыток мошенничества вследствие автоматизации преступных техник. Пора уходить от попыток персонально защитить только клиента или рассматривать в качестве объекта только банк. Необходима реализация подхода по защите всех участников процесса, своевременному обнаружению подозрительных действий и адаптации защитных мер в процессе возрастания рисков. Пришло время проактивной защиты!

В большинстве случаев клиент не знает, что он стал объектом повышенного внимания среди мошенников. Одно дело, когда клиента информируют о существующих рисках при работе в системе дистанционного банковского обслуживания, одинаковых для всех. Совсем другое дело, когда клиенту сообщают о доступности лично его данных (логине, пароле, криптографических ключах) на рынке кибепреступности или о том, что на его ПК зафиксирована активность, характерная для банковских вирусов. Наличие подобной информации может резко повысить сознательность клиента и позволит банку более адекватно принять решение по подозрительной транзакции.

Осознав необходимость модернизации подходов в борьбе с мошенничеством, компания Фродекс предложила рынку новый сервис FraudTrack, объединяющий усилия банка, клиента и профессионалов рынка информационной безопасности в борьбе с мошенничеством.

Традиционным системам антифрода не хватает информации о том, что происходит на стороне клиента и тем более о деятельности мира киберпреступности. Сервис FraudTrack призван устранить эти недостатки.

Сервис FraudTrack – это объединение уникального опыта и усилий специалистов компании Фродекс и признанных лидеров рынка информационной безопасности: ЗАО Лаборатория Касперского, компания Group-IB, компания IBM. Новая парадигма защиты уходит от противодействия мошенникам силами только лишь финансовой организации и реализует объединенную инфраструктуру борьбы с интернет–мошенничеством с участием финансовой организации, провайдеров-поставщиков оперативной информации о компрометации устройств и учетных данных клиентов, а также клиентов финансовой организации.

В сервисе FraudTrack к системе анализа информации FraudWall от компании Фродекс, имеющейся на стороне банка, добавляется облачная бесклиентская технология обнаружения враждебной активности на стороне клиента. Главная задача второго уровня защиты – по косвенным признакам обнаружить воздействие на устройстве клиента на типичный процесс работы в системе ДБО со стороны вирусного программного обеспечения или удаленное управление устройством. Добавив информацию о скомпрометированных учетных данных, ставшую известной в процессе традиционной борьбы на вирусном фронте, получим дополнительный канал информации о статусе клиента для принятия решений банковской системой антифрода. Немаловажно то, что технология не требует установки дополнительного программного обеспечения на стороне клиента, что позволяет начать её применять одномоментно для всей массы клиентов. При этом сервис FraudTrack обеспечивает банкам возможность выбора поставщика оперативной информации, например, это может использовать Bot-Trek Intelligent Bank от компании Group-IB.

Допустим, отработала связка первого и второго уровней защиты, банк выявил мошеннический платёж, клиент знает, что его ПК не безопасен. Что делать дальше? Дальше банк может проявить инициативу и предложить клиенту персональную защиту! Третий уровень защиты – это клиентское программное обеспечение, призванное обеспечить доверенную среду на устройстве клиента при работе с банковскими сервисами. Защита от утечки, перехвата и подмены банковских данных, более полный контроль состояния системы и защита от фишинга – далеко не полный перечень того, что позволяет клиенту спокойно работать, а банку – держать ситуацию под контролем.

Добавив возможности информационного обмена с облаком поставщика оперативной информации и контроля работоспособности со стороны банка, получаем третий полноценный компонент сервиса FraudTrack. Примером такого решения может быть Kaspersky Fraud Prevention for Endpoints от компании ЗАО «Лаборатория Касперского».

Итак, объединив усилия нескольких компаний, специализирующихся на отдельных аспектах информационной безопасности, мы предлагаем концептуально новую систему. Применяя сервис FraudTrack, банки смогут точнее выявить мошеннический платёж и получить актуальную информацию о состоянии клиентов с точки зрения информационной безопасности и об актуальных угрозах для клиентов и себя в целом. И самое главное, банк получит инструменты управления доверием к информации, поступающей от клиента.