Юрий ПРОКОФЬЕВ
Надежда КОВЕШНИКОВА

Эффективная система защиты, как правило, является многоуровневой, и каждый последующий уровень усиливает систему в целом. Такой подход позволяет каждому из слоев защиты сфокусироваться на своей конкретной задаче, а в случае необходимости можно заменить один слой другим. Как можно осуществлять сбор информации об устройстве, с которого клиент взаимодействует с банком по системе ДБО, для предотвращения мошенничества? Какие техники машинного обучения помогают определять мошенническую активность?

Юрий ПРОКОФЬЕВ, *компания «Фродекс», аналитик*
Надежда КОВЕШНИКОВА, *компания «Фродекс», аналитик*

Мониторинг клиентских устройств как средство повышения эффективности антифрод-систем

В настоящее время большая часть банковских антифрод-систем использует классический подход к обнаружению мошеннических действий. Такой подход основан на экспертной оценке и ручном анализе мошеннических операций. К примеру, в банк может поступить жалоба от клиента, который заявляет, что у него со счета пропали денежные средства. Такая жалоба может говорить о том, что появился новый вид мошенничества, который еще не знаком антифрод-системе. После того как эксперты поймут, как работает новая мошенническая схема, к правилам, используемым в системе антифрода, будет добавлено новое правило, применимое к выявленной «уловке» мошенников.

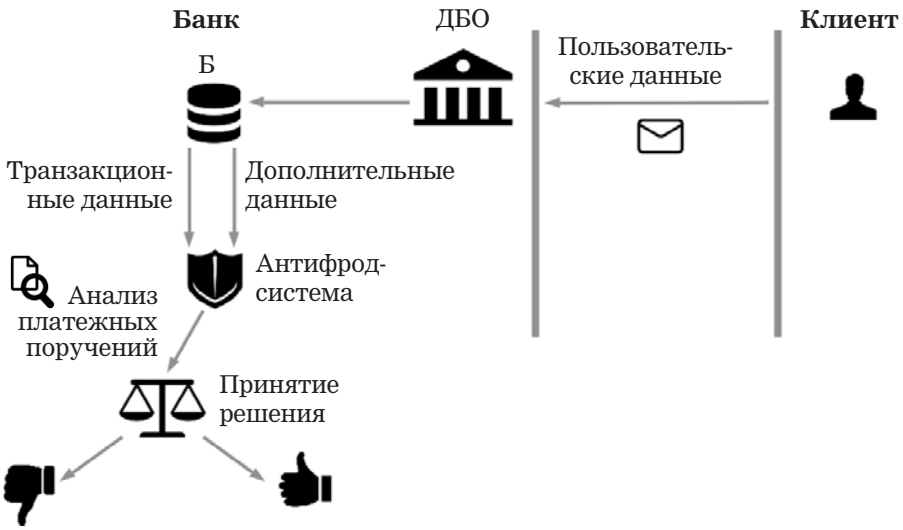
В общем случае в правилах используется схема условий «ЕСЛИ — ТО», и в качестве примера можно привести следующее правило: «ЕСЛИ сумма перевода более 1 млн руб. И сейчас ночное время, ТО выставить флаг “Мошеннический платеж” И оповестить ответственное лицо».

На рис. 1 изображена примерная схема взаимодействия пользователя с банковской системой: пользователь подключается к системе

Мониторинг клиентских устройств как средство повышения эффективности антифрод-систем

Рисунок 1

Общая схема работы антифрод-системы в банке



ДБО, авторизуется, формирует платежное поручение. Далее банковская система, как и антифрод-система, установленная в банке, работает только с полученными от пользователя данными. Система антифрода принимает решение, является ли данная операция мошеннической, на основе полученных данных, которые в общем случае можно разделить на транзакционные (информация непосредственно по платежу: куда перевести, сколько перевести и т.д.) и дополнительные (время осуществления перевода, IP-адрес клиента, MAC-адрес, поведение пользователя в системе и т.д.).

Безусловно, такие системы имеют очевидные недостатки:

— их дорого содержать, ибо они требуют постоянной ручной работы экспертов;

— чтобы правила успешно срабатывали на мошеннических операциях, а ложных срабатываний было меньше, правила необходимо постоянно корректировать.

Стоит отметить, что такая система использует опыт прошлого и не способна выявить новые мошеннические схемы. А ввиду того что мошенники постоянно придумывают новые способы «увода» клиентских денег, такой недостаток является значительным. Использование иного подхода к выявлению мошенничества в дополнение к классическому может существенно повысить степень обнаружения

Юрий ПРОКОФЬЕВ
Надежда КОВЕШНИКОВА

мошеннических операций и понизить количество ложных срабатываний.

Чего не хватает для составления полной картины?

Как уже было сказано, банковская система работает только с теми данными, которые ей передает пользователь. Банку ничего не известно о том, кто на самом деле передает эти данные: сам клиент сформировал платеж или кто-то просто заполучил логин и пароль и пытается похитить деньги клиента. Любой антифрод-системе не хватает знания о происходящем на стороне клиента для принятия более точных решений.

Банки, к сожалению, не могут или просто не отслеживают изменения поведения типовых мошеннических схем в отличие от компаний, специализирующихся на борьбе с мошенничеством. Если четыре года назад большая часть мошеннических платежей была сформирована вирусными программами, суммы переводов были небольшими и мошеннические платежи носили массовый характер, то за последние три года особую популярность у мошенников приобрело удаленное подключение к компьютеру жертвы. Однако сложность реализации атаки привела к снижению числа попыток и, как следствие, более качественной предварительной подготовке и переводам в куда более крупном размере.

И тот, и другой сценарии сопровождаются ключевыми признаками на стороне устройства клиента, отслеживание которых на стороне банка позволило бы качественно улучшить обнаружение неправомерных платежей.

Рассмотрим наиболее актуальную мошенническую схему сегодняшнего дня с применением социальной инженерии: мошенники звонят пользователю, представляются сотрудниками банка и под различными предлогами просят предоставить логин и пароль для подключения к системе ДБО (хотя получение логина и пароля может быть осуществлено и иными фишинговыми техниками). Затем, используя полученную информацию, мошенники подключаются к ДБО и осуществляют перевод, причем коды подтверждения реальный пользователь передает им сам в процессе общения. Деньги ушли. Если бы у банка была дополнительная информация о том, с какого устройства совершался перевод, было ли это устройство ранее замечено в мошеннической деятельности, является ли это устройство частью бот-сети и осуществляется ли на этом устройстве подделка каких-либо атрибутов, то исход мог бы быть иным.

Мониторинг клиентских устройств как средство повышения эффективности антифрод-систем

Так, за январь–май 2016 г. кибермошенники выведали данные банковских карт у 64 тыс. россиян с помощью классического обмана и социальной инженерии.

Знание того:

— в каком окружении находится пользователь системы;

— что происходит на момент формирования платежного документа,

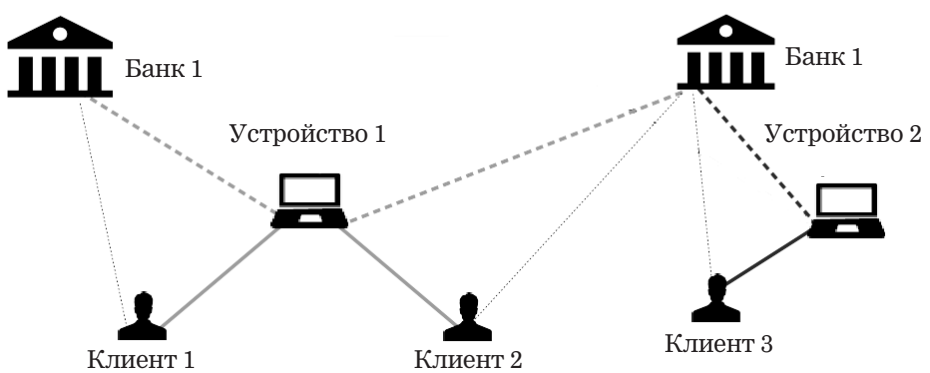
позволило бы в значительной степени повысить эффективность выявления мошеннических действий еще до того, как данные будут переданы в банк.

На рис. 2 изображено взаимодействие клиента с системой ДБО. Устройство, на котором работает пользователь, является посредником и представляет самого клиента. Человек может являться клиентом как одного, так и другого банка, но устройство использовать одно и то же. И наоборот, у клиента может быть несколько устройств, используя которые он может взаимодействовать с одной и той же системой ДБО. Именно клиентское устройство должно являться объектом наблюдения и сбора информации. Известны случаи, когда злоумышленники в сговоре с сотрудниками операторов сотовой связи перевыпускали SIM-карты жертв и использовали их на других мобильных устройствах для осуществления денежных переводов через системы мобильного банкинга. Как правило, после нескольких подобных смен SIM-карты устройство выбрасывается или перепродается.

Если система мониторинга обнаружит на устройстве мошенническую активность, то такое устройство будет помечено как мошен-

Рисунок 2

Взаимодействие клиентов с системами ДБО



Юрий ПРОКОФЬЕВ
Надежда КОВЕШНИКОВА

ническое. Банк, с системой ДБО которого это устройство начнет взаимодействовать, будет проинформирован о ненадежности такого устройства еще до того, как будут введены логин и пароль клиента.

Зачем следить и за чем следить?

Для взаимодействия с ДБО используются два вида устройств: стационарные ПК и мобильные. Если со стационарных компьютеров можно собрать информацию об их состоянии и характеристиках, то со вторых, помимо информации о самом устройстве, можно получить еще информацию и о реальном окружении пользователя, таком как окружающие точки доступа, GPS-координаты и пр. Для мобильных устройств такой вариант приемлем, так как банки стараются выпускать мобильные приложения для работы со своими сервисами, а интеграция модуля сбора информации с приложением, запускаемым на мобильном устройстве, позволяет получить более полную информацию об этом устройстве.

Куда сложнее осуществить сбор информации с персональных компьютеров: установка дополнительного программного обеспечения в большинстве случаев неприемлема, так как требует дополнительных действий со стороны пользователя, да и далеко не все согласны устанавливать на свой компьютер сторонний софт.

Взаимодействие клиента с интернет-банкингом осуществляется при помощи браузера. Сбор информации о системе пользователя через браузер, в свою очередь, является весьма привлекательным по ряду причин:

— возможность формирования уникального отпечатка устройства;

— возможность обнаружения мошеннической или вирусной активности, а также удаленного подключения;

— отсутствие необходимости устанавливать дополнительное программное обеспечение на стороне клиента;

— кросс-платформенность решения.

Формирование электронного отпечатка необходимо для сбора статистики по действиям, совершенным с устройства, и возможности отличать одно устройство от другого. В качестве примера можно привести способ формирования уникального отпечатка браузера на основе элемента HTML5 — canvas (Canvas Fingerprinting). Этот элемент используется для создания растрового двухмерного изображения при помощи различных скриптов. Алгоритм формирования отпечатка следующий:

1) браузер, выполняя указания из загруженного javascript'а, отрисовывает скрытый текст в виде картинки, используя элемент canvas;

2) отрисованная картинка будет немного отличаться от браузера к браузеру. На формирование изображения влияют многие факторы, в том числе настройки браузера, операционная система и физические компоненты компьютера;

3) картинка, пиксель за пикселем, конвертируется в строку, закодированную в base64. Полученная закодированная строка будет уникальной почти для каждого браузера.

Для более точного формирования отпечатка помимо атрибутов, полученных из браузера, можно использовать информацию о состоянии сетевого соединения, реализации стека TCP/IP на устройстве, что в случае подмены заголовка User-Agent может дать более точную информацию об операционной системе, используемой на устройстве.

Система контроля пользовательского окружения должна определять изменения, касающиеся одного и того же устройства. Предположим, пользователь установил новый плагин, что повлияло на отпечаток того окружения, в котором он работает: система контроля должна уметь выявлять подобные изменения и обновлять уникальный идентификатор устройства вместо создания записи о новом устройстве.

Определение аномального поведения на стороне пользователя может сигнализировать о мошеннической активности.

К аномальному поведению можно отнести:

— сеанс удаленного подключения;

— запросы к сторонним ресурсам, что может быть следствием успешной XSS-атаки или внедрения мошеннического кода;

— появление поддельных DOM-элементов на странице;

— подмена атрибутов браузера.

Big Data и выявление мошенничества

Выявление нового вида мошенничества, как правило, занимает некоторое время. Сначала проявляется результат мошеннической операции, затем проводится расследование для определения новой схемы. После этого к правилам, используемым в системе, добавляется новое правило, и чем скорее это правило появится, тем быстрее антифрод-система начнет обнаруживать мошеннические операции.

Новые мошеннические схемы достаточно быстро распространяются среди «своих». Это увеличивает частоту их использования, что, в свою очередь, влияет на скорость их выявления.

Для своевременного обнаружения новой мошеннической активности необходимо организовать сбор и обработку большого количества данных. Система сбора, хранения и анализа полученной информации должна представлять собой облачное решение. Разво-

Юрий ПРОКОФЬЕВ
Надежда КОВЕШНИКОВА

рачивание такой системы на стороне банка будет крайне неэффективным по нескольким причинам:

— высокая эффективность анализа зависит от количества собранной информации по устройствам. Развернутой обособленно в банке системе не будет хватать данных;

— содержание подобной системы потребует от банка выделения значительного количества ресурсов: на закупку дорогостоящего оборудования, администрирование, обучение инженеров и пр.

Благодаря большому объему собранной и проанализированной информации каждый банк будет оперативно получать информацию о новых мошеннических устройствах.

Стоит обратить особое внимание на то, что собираемая информация имеет отношение только к устройствам пользователей систем ДБО. Никакая информация по самим клиентам банка не требуется.

Техники определения мошеннической активности с использованием машинного обучения

Можно привести следующие примеры техник, применяемых для анализа больших обьемов данных:

— техника обучения «без учителя» (unsupervised learning), целью которой является поиск отклонения от нормального состояния. Такая техника использует исторические данные и не требует определений того, какие показания считать мошенническим поведением, а какие нет. Сразу стоит заметить: отклонение от нормального поведения не значит, что это мошенническая активность. Такая техника позволяет выявить новые мошеннические схемы;

— техника обучения «с учителем» (supervised learning). Целью такой техники являются работа с информацией, полученной из исторических данных, для получения образцов мошеннического поведения и дальнейшее применение полученных «знаний» для выявления схем, используемых мошенниками, в потоке новых поступивших данных. Поскольку феномен мошенничества динамический и мошенники часто находят новые лазейки, такой подход оказывается бессильным для выявления новых схем обмана, но хорошо справляется с поиском «по образцу».

Перечисленные типы дополняют друг друга, так как каждый из них работает с отдельным аспектом мошенничества.

Выводы

На текущий момент до 95% краж средств клиентов связано с фродом в интернет- и мобильном банкинге, поэтому данному типу атак

Мониторинг клиентских устройств как средство повышения эффективности антифрод-систем

следует уделить наибольшее внимание. Ведь только за январь–май число интернет-краж с банковских карт достигло 28,5 тыс. случаев, что на 42,5% больше показателя за пять месяцев 2015 г. Следует отметить, что с ростом количества операций растут и потери, которые за указанный период 2016 г. составляют порядка 3,5 млрд руб., что почти в 2 раза больше, чем в 2015 г.

Система контроля окружения пользователя является отличным дополнением к уже имеющимся антифрод-системам, используемым в банках. Помимо раннего выявления мошеннической активности, такая система поможет снизить количество ложных срабатываний, что приведет к снижению нагрузки на банковских операторов, осуществляющих обзвон клиентов для подтверждения совершения операции. В свою очередь, это приведет к снижению банковских затрат. Как следствие, повысится лояльность клиентов: их будут меньше беспокоить просьбами подтвердить ту или иную операцию.

Такие системы уже на протяжении нескольких лет используются зарубежными банками. Об успешности данного подхода свидетельствует тот факт, что в этом году Сбербанк начал использовать подобную систему для повышения уровня безопасности своего интернет-банкинга.