Мошенничество на сетях связи

Антон ЗАРУБИН,
доцент, СПбГУТ

Юлия СЕДОВА,
инженер, МОУ ДОД ЦИТ

Статистика, существующая по разным типам фрода, различается от источника к источнику, но порядок чисел остается весьма серьезным. Так, общие потери операторов связи от деятельности злоумышленников составляют 1–7% доходов операторов связи от предоставления телекоммуникационных услуг [1, 2]. Кроме того, с увеличением объемов предоставления телекоммуникационных услуг и выручаемых за это средств, растет и абсолютная величина доходов мошенников. Относительное изменение доли потерь операторов от фрода также выражается возрастанием, наиболее заметным на активно развивающихся телекоммуникационных рынках.

Способы и схемы мошенничества

Способы мошенничества весьма разнообразны и отличаются своими долями в общей массе. Так, по количеству инцидентов лидируют разновидности фрода, связанные с контрактами между оператором сети и пользователем (subscription fraud), на их долю приходится около 40% всех случаев. Мошенничество с номерами prepaid-карт составляет примерно 9% случаев, а приблизительно в 8% случаев всех злоумышленных действий в них оказываются вовлечены сотрудники пострадавшего оператора связи (internal fraud). С точки зрения финансовых потерь самое опасное именно инсайдерское мошенничество – на него приходится около 40%, потери от остальных типов фрода находятся в области 10%. Приведенная статистика является лишь оценочной, так как типы фрода и его схемы зачастую пересекаются и далеко не всегда поддаются точной классификации.

Отдельного внимания заслуживает тема эволюции видов, схем и средств телекоммуникационного мошенничества. При кратком анализе здесь складывается следующая картина: с развитием и усложнением телекоммуникационных систем и услуг, а также с увеличением количества операторов связи аналогичный процесс происходит и со схемами фрода. Если в первой половине XX в. основные типы телефонного мошенничества представляли собой незаконное подключение к линиям фиксированных сетей связи с целью получения услуг связи или прослушивания разговоров, то с появлением электронных УПАТС и средств компьютерной телефонии в 1970–1980 гг. операторы столкнулись со злоумышленным вмешательством в схемы учета объемов предоставленных услуг связи и взломом учережденческих станций.

Следующим шагом на этом эволюционном пути в 1990-х гг. стало появление мошеннических схем, связанных особенностями тарифов на пропуск трафика и работой биллинговых систем операторов, «клонированием» мобильных телефонов, подменой идентификаторов абонентов и терминалов. Далее, 2000-е гг. ознаменовались распространением средств VoIP, что обеспечило злоумышленников новыми

прибыльными схемами по пропуску трафика, а также позволило успешно паразитировать на новых операторах связи. Наконец, в текущий период времени, характеризующийся конвергенцией сетей и услуг связи, появляются свои конвергентные формы мошенничества. И простой компьютерный вирус, требующий от пользователя отправить SMS-сообщение на премиум-номер, чтобы разблокировать его компьютер, – только начало этого эволюционного отрезка.

На этом фоне универсальной уязвимостью оператора связи становится отсутствие понимания сложившейся в данной области ситуации и постоянного контроля над ней, что особенно актуально для небольших операторов связи. Все остальное – лишь частные случаи, которые могут быть решены реализацией превентивных организационно-технических мер или своевременным обнаружением факта мошенничества.

В общем случае схема действий злоумышленников включает следующие объекты: операторы связи, конечные пользователи телекоммуникационных услуг (физические или юридические лица), сам злоумышленник. При этом в роли мошенника могут выступать как операторы или пользователи, так и третья сторона. В зависимости от распределения ролей и присутствия в схеме тех или иных объектов схемы мошенничества, рассмотрим примеры некоторых типов фрода:

- абонентское мошенничество – мошенничество, совершаемое третьей стороной в отношении абонента сети связи или пользователя телекоммуникационной услуги. Схемы такого рода действий направлены в основном против физических лиц – пользователей терминалов сетей связи;
- операторское мошенничество, при котором усилия злоумышленника направлены напрямую против оператора связи;
- инсайдерское мошенничество, когда злоумышленник использует те или иные ресурсы оператора, что приводит к прямым финансовым или косвенным потерям.

Приведенная классификация не является четкой и используется авторами в рамках данной статьи, для более детальной классификации мы рекомендуем обратиться к источнику [1].

Абонентское мошенничество

Абонентское мошенничество наносит серьезный косвенный ущерб оператору, который может выражаться в увеличении дебиторской задолженности, ухудшении имиджа компании и даже в потере вполне дисциплинированных пользователей. В прошлом оно оставалось в рамках подключения злоумышленника к чужой телефонной линии или кражи номеров предоплаченных карт, сегодня же, благодаря развитию коммуникационных технологий и появлению ряда новых услуг, оно получило «новое дыхание».

Вот типичный пример новостного релиза одного из крупных операторов подвижной связи: «Вирус распространяется под видом бесплатного программного обеспечения для мобильных телефонов. На телефон устанавливается специальный файл, позволяющий автоматически осуществлять выход в Интернет, обращение к стороннему серверу для определения префикса, отправку SMS и его удаление из списка отправленных SMS-сообщений» [4].

Сегодня большинство сценариев абонентского мошенничества опирается на методы социальной инженерии, но при этом его нельзя назвать низкотехнологичным, в отличие от традиционного случая с «выманиванием» номеров предоплаченных карт. В борьбе с такого рода фродом единственно эффективными оказываются организационные меры, направленные на информирование абонентов о возможных угрозах, и организационно-технические механизмы оперативной блокировки ресурсов злоумышленников. Крупные операторы подвижной связи, работающие на российском рынке, предпринимают целый ряд мер для защиты от мошенничества, направленного на абонента. Это выражается в появлении весьма информативных ресурсов о существующих угрозах и ужесточении требований к работе контент-провайдеров. Читатели, интересующиеся актуальными видами абонентского мошенничества, могут обратиться к источникам [4, 5, 6].

Михаил БАШЛЫКОВ, руководитель направления информационной безопасности компании КРОК

Проблема мошенничества сегодня очень актуальна для компаний финансового сектора. Банки теряют деньги, свои и своих клиентов, причем угроза исходит как от внешних злоумышленников, так и от внутренних. Во многом это обусловлено сложностью контроля действий банковских работников в АБС, а также активно растущим объемом услуг дистанционного банковского обслуживания. Безусловно, это влечет риск совершения мошеннических операций третьими лицами, которые тем или иным способом получают доступ к счетам клиентов. Все это наносит ощутимый ущерб банкам в виде потерянных клиентов, испорченной репутации, судебных исков, штрафов и т. д. Для предотвращения подобных случаев мы предлагаем банкам усовершенствовать технологии предоставления дистанционного доступа к счетам, реализовать системы контроля и анализа операций клиентов, операторов и работников банка. К примеру, сейчас мы строим для крупного российского банка аутентификационный центр, позволяющий различать десятки тысяч клиентов ежедневно не только на основе пароля и логина, но и с помощью встроенных в платежные карты микрочипов.

Иногда сложные механизмы доступа могут быть обременительны для клиентов, поэтому мы предлагаем также использовать технологии поведенческого анализа. По мере того, как действия клиента отклоняются от привычного для него шаблона поведения, включаются новые уровни аутентификации, задаются дополнительные вопросы и т. д. Этот механизм также успешно используется в борьбе с внутренними мошенниками. К примеру, когда операторы банка, пользуясь своим служебным положением, интересуются информацией о счетах VIP-клиентов или распоряжаются средствами неактивных счетов. Наш опыт внедрения поведенческого анализатора в представительстве иностранного банка доказал его эффективность, с помощью этого инструмента был выявлен целый ряд нарушений.

мнение специалиста

Кирилл ЛЬВОВ,
менеджер по развитию бизнеса компании «Verysell Проекты»

Наиболее эффективным способом защиты от телефонного мошенничества являются системы Fraud Management System. С их помощью оператор получает возможность фиксировать в режиме on-line случаи пропуска несанкционированного трафика под видом клиентского и предупреждать об этом своих абонентов. И отечественные, и зарубежные продукты постоянно развиваются. Системы совершенствуются по трем основным направлениям: увеличение производительности (в связи с постоянным ростом объемов обрабатываемой информации), удобство использования (для снижения квалификационных требований к обслуживающему персоналу), адаптация к новым системам и услугам связи. Сейчас перед разработчиками FMS стоят новые задачи: им необходимо уберечь от мошенничества абонентов и операторов сетей 3G и спутниковых систем связи.

Основными функциональными возможностями современных систем FMS являются: анализ детальных записей о вызовах и другой информации с применением современных алгоритмов, набор методов выявления мошенничества для различных категорий связи и услуг: ТфОП, GSM, GPRS, 3G, VoIP, dial-up и др., передача информации в аварийную службу и оповещение заданного списка пользователей для ускорения реакции на действия мошенников, ведение «черного списка» лиц, уличенных в мошенничестве, интеграция со сторонними CRM- и биллинговыми системами.

Операторское мошенничество

В качестве инициатора операторского мошенничества могут выступать абоненты сети, сопряженные операторы, партнеры или сторонние компании. В первом случае можно привести следующие примеры фрода:

- использование контрактов с физическими лицами для подключения корпоративной сети. В этом случае оператор может терпеть ущерб за счет разницы в тарифах на обслуживание физических лиц и подключения офисной АТС. Подобные действия злоумышленников могут определяться при помощи анализа загрузки абонентских линий;
- использование услуг связи без намерения их оплаты. Из-за особенностей работы механизмов биллинга этот вид мошенничества доставит серьезный ущерб, особенно если речь идет о предоставлении услуг связи абоненту, находящемуся вне пределов домашней сети. Методы защиты от действий подобного рода – применение механизмов предоплаченного биллинга в реальном времени и наблюдение за паттернами абонентской нагрузки.

Сценарии злонамеренных действий со стороны сопряженных операторов зачастую работают за счет особенностей тарифов на пропуск трафика между операторами и могут включать, например:

- мошенничество с подменой идентификаторов вызываемых абонентов с целью представления междугородных и международных вызовов как местных;
- зацикливание вызовов, приносящее доход мошеннику за счет разницы в стоимости обработки вызова между ним и оператором-объектом мошенничества. Оба этих сценария могут быть обнаружены при анализе CDR-записей коммутаторов или данных систем мониторинга ОКС № 7;
- незаконное вливание трафика, при котором недобросовестный оператор приводит свой МГ/МН-трафик в сеть другого оператора, например, через шлюз IP-телефонии, установленный в местной сети под видом учрежденческой АТС;
- обратная схема, когда оператор местной сети связи приводит МГ/МН-трафик, пользуясь случайными или злонамеренными ошибками в конфигурации шлюзового оборудования сопряженного оператора;
- установка на собственной сети сервисной платформы голосовых услуг под видом УПАТС.

мнение специалиста

Андрей СВИРЩЕВСКИЙ,
руководитель направления департамента продаж, компания SAS Russia/CIS

Среди внутреннего мошенничества также следует отметить неоптимальную маршрутизацию трафика на присоединенных операторов: вызовы терминируются не напрямую на оператора вызываемого абонента или соответствующего оператора дальней связи, а на связанного с мошенником другого оператора. Тогда услуга при взаиморасчетах может быть, например, не «зоновое завершения вызова на сеть присоединенного оператора связи», а «зоновое завершение вызова на сеть другого оператора связи», т.к. возникает лишний транзит трафика. Стоимость «зонового» транзита может составлять, например, 38 коп. за минуту. В масштабах миллионов минут в месяц это может приносить существенные потери. Такая ситуация часто возникает при перегрузке основного канала маршрутизации и задействовании резервного канала, но также может быть следствием мошеннических действий. Выявляется данный вид мошенничества статистическим анализом терминируемого вовне трафика путем сопоставления номерных емкостей вызываемых абонентов, интерконнект-услуг и присоединенных операторов, на которых терминируется трафик.

Инсайдерское мошенничество

Инсайдерское мошенничество предполагает, что злоумышленник, действующий изнутри операторской компании, использует доступные ему технические, информационные или административные ресурсы для продажи их в обход компании или для выстраивания более сложных схем. Авторы могут привести следующий наглядный пример.

Сотрудник провайдера телефонных услуг (аналог сервиса «виртуальны офис»), имеющий права на конфигурацию параметров клиентских учетных записей и учетных записей сотрудников провайдера,

создает целый ряд подобных записей и отмечает их как служебные аккаунты сотрудников компании. Затем он продает доступ к ресурсам этих учетных записей сторонним лицам. Злоумышленники пользуются предоставленными ресурсами для совершения телефонных вызовов на премиум-номера, зарегистрированные сторонними операторами в ряде стран. Вызовы с учетных записей, созданных злоумышленником, передаются на ограниченный ряд премиум-номеров, предположительно созданных той же группой злоумышленников. Провайдер телефонных услуг терпит убытки, а деятельность мошенников обнаруживается только после анализа аномального увеличения количества телефонных вызовов на редко используемые направления.

Главной особенностью сложных схем операторского мошенничества является то, что для каждого конкретного случая они имеют свои уникальные детали, основанные на нюансах работы того или иного оператора, схемах его тарифов и тарифов сопряженных операторов, определенных недочетах в конфигурации коммутационного или шлюзового оборудования. Субъективный опыт позволяет говорить, что подобное мошенничество – довольно редкое явление на сетях операторов, однако приводит к весьма ощутимым потерям, особенно когда в этом замешаны собственные сотрудники оператора.

Противодействие мошенничеству

Каким образом можно противостоять угрозам, подобным рассмотренным выше? Как уже упоминалось, самым важным шагом в этом направлении должно стать понимание оператором связи существующих рисков и рисков ближайшей перспективы, которое было бы персонифицировано в соответствующих кадрах компании. Именно перед ними должна стоять задача выполнения типовых проверок безопасности сети связи и разработки алгоритмов контроля за новыми услугами и процессами, вводимыми в компании. Причем эта работа может вестись как самостоятельно внутри компании, так и с привлечением поставщиков FMS.

> Существующие решения на базе FMS повышают эффективность поиска или предотвращения фактов мошенничества.

В заключение хотелось бы отметить, что существующие решения на базе FMS, несомненно, повышают эффективность поиска или предотвращения фактов мошенничества, особенно когда дело касается обработки больших объемов информации, сравнения паттернов трафика или автоматической сигнализации о появляющихся аномалиях. Вместе с тем, множество таких задач, как обнаружение нетипичных потоков трафика, корреляция списков активной и переданной пользователям номерной емкости, выявление аномально возросшей интенсивности расхода средств на предоплаченных учетных записях и т. п., могут быть решены подручными средствами и минимальной скриптовой автоматизаций.

Это подчеркивает тот факт, что в контексте борьбы с фродом в связке «замечательный инструмент – мастер, понимающий принципы его работы» главным остается все-таки последний. ■

Литература

1. Telecommunication Fraud Management. Stephen Brown, 2005. www.waveroad.ca
2. *Голышко А.* Преступные сети для телекоммуникационных операторов // Connect! Мир связи. 2010. № 1.
3. *Седова Ю.* Мошенники в «паучьих» сетях // Connect! Мир связи. 2007. № 5.
4. http://stopfraud.megafon.ru
5. http://safe.beeline.ru
6. http://www.mts.ru/safety