Операторский фрод – всем выгодно?

Читая о том, что якобы ужесточение мер по борьбе с киберпреступниками, использующими короткие SMS-номера, обернулось для операторов потерями выручки от направления контент-услуг, теряешь сон и очень сильно переживаешь. Ведь, просматривая такие тексты, операторы "Большой тройки" кажутся нам такими идеальными ангелами в белых одеждах, которые одной рукой исцеляют страждущих, а другой даруют им услуги связи за сущие копейки. На самом деле, такое впечатление у журналистов, а после и у читателей, складывается, если слушать только пресс-службы операторов связи и общаться с тщательно подготовленными спикерами их управляющих "надстроек". Как только даешь себе труд "копнуть" глубже - можно найти много интересного.

И вечный бой?

Для начала определимся с терминами. По классификации Всемирной Ассоциации GSM, существует примерно 200 видов мошенничества в сотовых сетях, которые можно разделить на три основные категории. Во-первых, это деятельность абонентов, всячески уклоняющихся от уплаты по счетам. Во-вторых, техническое мошенничество - вмешательство в ИТ-системы оператора сотовой связи с помощью специальной аппаратуры и программного обеспечения. И, наконец, в-третьих, мошенническое использование SIM-карт. Эта категория объединяет два типа преступления. Использование рассылок, вирусов, троянов для обмана пользователей с целью получения денег от них. И второй тип - мошенничество, основанное на программных "дырах" операторов связи.

Для получения точной информации мы поговорили об этом с несколькими сотрудниками отделов информационной безопасности крупных операторов связи и выяснили, как же обстоит дело на самом деле. Как известно, от фрода страдают только две категории участников рынка - это сами операторы связи и их абоненты. Временами "под раздачу" попадает еще дилер, но это экзотика.

А вот количество тех, кто обманывает - куда как больше. "Жульничает, во-первых, сам оператор связи, - говорят нам наши собеседники. - Тут полная свобода - навязывание различных услуг, снижение порога отключения, что дает возможность "падать в минус" для абонента и т.д. Отделам безопасности достается и от абонентов - история о "деле на миллион" это классический случай. Может быть еще круче - множество карт, которые звонят на платные номера в роуминге, а от абонента мы получаем заявление о непричастности. Разумеется, "в деле" могут быть и дилеры операторов сотовой связи - они "резвятся" с подключениями. Наиболее часто встречаются множественные подключения - когда человек приходит в салон, у него берут копию паспорта. Он подключает себе номер, а потом на его паспорт ещё симки вешают. На некоторых "героев" приходится по тысяче контрактов. Другой "одаренный" оператор, не дилер даже (!) формировал специальные пакеты копий паспортов и "гонял" их для массовых подключений по 4 соседним областям - эти симки раздавали буквально даром в метро, на рынке и по различным акциям. Ну и не будем забывать настоящих жуликов - там есть любители и профи. Последняя категория, как мы понимаем, уже "квартирует" в исправительно-трудовых колониях - они практически монопольно занимаются "разводами", лотереями, розыгрышами призов, а также специализированными разводами (к примеру, для таксистов). Есть и любители - обычно студенты и школьники, которым просто нечего делать".

По факту оператор борется только с фродом в отношении себя, до всех остальных, мягко говоря, им нет никакого дела. "Разговоры о том, что компания заботится о своих абонентах, на самом деле, можно оценить. К примеру, у какой компании работают автоматизированные системы возврата абонентам денег по фроду со стороны контент-мошенников в превентивном порядке? Ни у кого нет. Вот и реальная "забота". Фактически, оператор по-настоящему борется только с фродом в отношении себя. На всех остальных им плювать слюной.. Какое дело компании до клиентов, когда у неё у самой потери бешенные... Бывают месяцы, когда операторы в России или странах СНГ теряют от действий злоумышленников миллионы (встречаются цифры в 2-4,5 млн. долл.) И как они это отражают на балансе?":)

Временами, а если точнее, то крайне иногда, операторы связи на уровне того или иного региона пытаются "быть хорошими" и внедряют системы выявления и локализации, пресечения фрода. Все подобные системы иностранного производства (полноценные аппаратно-программные комплексы), которые, тем не менее, необходимо "дорабатывать напильником". Но все они, как мы понимаем, защищают только оператора - о клиентах по-прежнему никто не думает. Что же запускают операторы?

Система множественных подключений - если на одного абонента оформляется больше 10 контрактов, то система их "видит" и маркирует такую активность как подозрительную. Не обязательно это мошенник, но проверить необходимо и такая заявка сразу ставится на контроль. Система "черных списков" - вариантов здесь много, используют наиболее простой вариант, когда данные о паспортных данных, с которыми работают мошенники, вносятся в систему и при попытки подключить к ней телефонный номер его активность блокируется - ни вызовы не совершить, ни SMS отправить, в т.ч. и на премиум-номер. Система слежения за мошенниками через SMS - весь трафик

"процеживается" с помощью фильтров, настроенных на ключевые слова, известные смысловые конструкции "разводов", что позволяет не только оперативно пресекать SMS-спам, но и выявлять установочные данные мошенников: по сути, можно сразу отдавать их правоохранительным органам. Система выявления клонов сим карт - кажется, это особенно объяснять не надо, идет установка по IMEI телефонов и дистанционное блокирование.

Были разработаны и поставлены в опытную эксплуатацию системы, которые "выбивали" целевой фрод. К примеру, для предотвращения атак со всевозможными конкурсами и "выигрышами", были определены конкретные ИТК из которых осуществлялось до 90% такого фрода. Была придумана интересная схема – «известно какие БС работают на территорию ИТК, кроме того только осужденные, со своими телефонами (которые по закону им в общем-то иметь никак нельзя!) не выходят за пределы этой территории. Количество телефонов на территории ИТК не бесконечно и их нельзя ввести пачками (в отличии от SIM-карт). Таким образом, можно установить какие мобильные аппараты находятся у мошенников. Дальше было разработано два основных сценария. Во-первых, от производителей телефонов мы узнали что существуют специальные коды, которые, если их передать в виде SMS, позволяют отключать телефон с разными эффектами от исчерпания батареи до выключения сети. То есть при "выходе на связь" телефонов злоумышленников их мгновенно бы отключали в автоматическом режиме с предоставлением отчета. :) Второй вариант был еще проще - превентивно отключать все симки, которые будут работать с IMEI телефонов мошенников после регистрации в сети. И что вы думаете, случилось дальше? Мы описали всю систему, готовы были ее показывать - отправили документы в столицу. Ответ пришел через неделю. Общий смысл такой - мошенники когда звонят и разводят «абонов» тратить деньги на связь. Значит, приносят оператору прибыль. Во внедрении - отказать. Точка», - с грустью говорят наши собеседники.

Борцы невидимого фронта

У всех операторов "Большой тройки" этим "крестовым походом" на мошенников, обычно, занимается два подразделения. Первые - подразделения из финансового блока и, соответственно, вторые – это службы безопасности. В свое время у некоторых операторов была хорошая идея сделать одно подразделение по фроду (к примеру, такое предложение формировали в "МегаФон" и отдать его в Службу безопасности"). Но так и не получилось. А ведь фрод мало выявить - надо найти мошенника. Что греха таить сотрудники МВД (да и частично ФСБ) не всегда хорошо представляют как работает связь. Технических терминов пугаются, особенностей функционирования сетей мобильной связи не знают даже на уровне просвещенного абонента. Как можно им работать в таких условиях? Всем надо помогать знаниями со стороны спецов оператора связи.

«Расследованием преступлений в сфере высоких технологий у нас занимаются... СБ тех игроков рынка, которым это больше всего надо, - комментируют наши собеседники. - Даже "самородка" преступного поймать зачастую крайне сложно, а труднее всего бороться с организованными группами, где есть специалисты в области сотовой связи: они и шифруются грамотно и схемы вывода денег практически идеальные придумывают. Так что если операторы связи говорят о том, что их задача только зафиксировать нарушение, расследованием которого будут заниматься правоохранительные органы, то здесь все, формально, правильно. Но если они все будут делать по закону и передадут дело в то же МВД без деятельного сопровождения процесса, то можно в нем ставить точку. На практике ОРД будет идти вяло - скинут дело какому-нибудь старлейту или капитану, он будет писать запросы, проводить экспертизы и т.д., а на это нужна куча времени. Часто сотрудники не могут даже экспертам, коли они у них все-таки есть, грамотно поставить задачу и вопросник составить: их квалификация низка. Большинство из них не знает даже базовых знаний о работе компьютерных сетей и сотовой связи, это не их вина.

СБ оператора сотовой связи формально не имеет право вести ОРД, но если не делать этого самим - ничего не произойдет. Поэтому, в лучшем случае, СБ ездит на мероприятия вместе с органами, а чаще просто оперативно проводит расследования своими силами и просто передает «коллегам в погонах» все материалы. Но о сотрудниках правоохранительных органов нельзя сказать, что они получают все готовое: ведь они все правильно оформляют. Задерживают подозреваемых, проводят очные ставки, звания за успехи получают, награды и премии. :) Кстати, в идеале сотрудник СБ оператора связи - это технарь с определенной "заточкой". Важно не знание по оформлению документации, а умение работать с людьми и выстраивать контакты с правоохраниетельными органами, кроме того - знание как работает связь». Видимо, здесь как в фильмах со Сталлоне - "Что бы поймать маньяка- нужен другой маньяк".

«К сожалению, - признаются опрошенные нами эксперты, - в настоящий момент борьба с фродом идет по принципу "работаем по заметным целям". То есть как только обозначается громадная проблема - значит мы бежим ее решать. Превентивно никто этим, по большей части, не занимается - как все мои коллеги сидели ровно, тихо, так до сих пор и сидят. И это при том, что обладая минимальными финансовыми ресурсами можно организовать в каждом макрорегионе такие технические возможности, которые б позволили пресекать фрод в зародыше. Да и "борцов" с фродом становится все меньше. Опять же уровень противодействия велик - когда человеку, который этим занимается у оператора связи, к домашней двери наступательную гранату привязывают, то хочется

ему после этого "глубоко копать"?

Кроме того, насчет фрода самого оператора - здесь двойственность. Вот вы борец с фродом. А сама компания делает все, чтобы этого фрода было много. Планы продаж такие, что все рынки и станции метро завалены симками. Вы идете к начальству и говорите: "Вот дилер симки на рынок сбросил с нарушениями, отсюда фрод - надо дилера "нагнуть". А вам говорят: "У нас план по подключениям - если мы дилера нагнем, то план не выполним. План не выполним - показатели квартальные (годовые) к черту пойдут. Показатели пойдут к черту - премии не будет. А по величине фрода у нас премии не раздают. Так что тебе это надо?" Вот и вся борьба».

Наши собеседники с грустью и скептическими улыбками встретили наши контраргументы о заявлениях операторов связи о том, что «им достаточно массовой жалобы (под этим понимается 3-5 однотипных обращений в день) и проблема ставится "на карандаш"». «Все может быть, - говорит один из опрошенных нами специалистов, - только, видимо, дальше "карандаша" дело не идет. Большинство массовых мошеннических акций можно было сбить еще в самом начале. Но НЕ нужно это. Или вот тезис операторов о том, что если вам в SMS-рассылке попадается телефон мошенника, то "звоните в call-центр и его заблокируют". Сообщать о таких номерах, конечно, имеет смысл. При том, что если бы оператор поставил себе систему не сканирования, а анализа SMS-спама, он бы сам эти номера видел мгновенно. Но что дальше? Оператор сам по себе не может взять и "погасить телефон". Он на это права не имеет. Придет владелец и спросит: "по какому праву?". А что ему ответить? "Вы обвиняетесь в мошенничестве?" :) Оператор сотовой связи не суд и не прокуратура.. И даже не милиция. Вот будет бумага из милиции - вопросов нет, блокируют. Но сами в превентивном порядке таких дел не инициируют.

Хотя, есть методы. Вот был у нас один прецедент - пришел человек написал заяву на выдачу денег с закрываемого номера (есть такая процедура). Начали проверять - уффф, а номер-то типичный "кошелек", где идет обнал денег по мошенническим схемам. Сдавать его в милицию? Самим дел других хватает. Просто послали мужика подальше. Он с адвокатом пришел - денег уж очень много было. Послали обоих. Сказали, что как только будет еще один заход, то связей хватит в милицию их сдать. Беспредел с нашей стороны, конечно. А какие еще варианты? Деньги они с номера перевели куда-то оперативно и наверно там обналичили. Но так работать постоянно нельзя. Пока абоненты по каждому факту мошенничества не начнут "автоматом" писать заявления в милицию, а милиция по ним работать - ничего не будет».

Специфика на примерах

На рынке существует несколько сотен примеров фрода – если разбирать каждый отдельно, надо писать книгу. Отметим самые показательные. Кстати, отличный вариант для весьма живучего фрода по коротким номерам - зарегистрировать множество SIM-карт на паспорт человека, который стоит на учете в психоневрологическом диспансере. И быстро зарядить их в специальный аппаратно-программный комплекс для отправки сотен SMS на короткие премиум-номера для обнуления счета и "загона" номеров в приличный минус: по контент-услугам операторы связи это делать позволяют. Если использовать всего один компьютер с одним мобильником, то можно отправить 50 SMS за полчаса. Для "обнала" используются фродовые сервисы "пополни WebMoney за SMS" - пусть даже клиент получает треть от переведенных денег. По условиям таких ресурсов за час с каждого номера можно отправить SMS не больше чем на 10-20 долл., поэтому для нормального заработка необходимо использовать целую пригоршню SIMок.

Особенность состоит в том, что при большом потоке платных SMS "бедные" серверы операторов связи дают абоненту упасть "в минус" больше, чем на 500 руб. для каждого абонентского номера. Отсюда и easy money. :) Судя по учебным фильмам МВД, «блокировка SIM-карты с отрицательным балансом наступает от 25 минут до 48 часов: вполне есть время, чтобы "набить" нужное количество платных SMS, иногда на несколько десятков тысяч рублей». Верится в это с трудом, но, видимо, это удается сделать в тот момент, когда на оборудовании оператора связи ведутся ремонтные работы и тарификация по премиум-номерам осуществляется с задержкой. Правда, для точной информации о таких технологических «окнах» нужна точная информация от ответственных сотрудников провайдера мобильной связи. Но это, как мы понимаем, не проблема.

Временами мошенники талантливо подстраиваются под рекламные активности операторов связи и, таким образом, при минимальной подготовке, могут заработать вполне интересные деньги. "В одном из регионов у меня был интересный случай, - вспоминает один из наших собеседников, - мальчик 16 лет придумал следующую схему: у МТС была акция по получению денег на счет за пополнение своего электронного счета у оператора связи. Так он "встроился" в эту рекламу просто отправляя SMS абонентам, номера которых брал в газете "Из рук в руки" - типа "отправьте смс с таким-то текстом на короткий номер и получите от МТС 100 руб на счет". Разумеется, текст содержал в себе код контент-провайдера и код клиента. Так он действовал пару недель - прилежно собирал номера из газеты в текстовый файлик, отправлял SMSки "руками", использовал аномайзер, анонимный кошелек для получения денег. А контент-провайдеру, для регистрации в партнерке, прислал заранее нарисованный в фотошопе паспорт российского гражданина. Получал, кстати, 30% от стоимости SMS.

Еле поймали - допустил всего одну ошибку и на этом его взяли. Правда, никакого наказания не понес - был болен эпилепсией".

Но если по такому же принципу работает преступная группировка, то результаты, конечно, выше. Яркий пример - у торговой организации, у которой есть дисконтные карты и дисконтные программы воруют базу клиентов: с фамилиями, именами и телефонами. Далее настраивают простенькую программу, которая раскидывает персональные SMS от имени этой торговой организации (вместо номера отправителя - название этой организации). Текст простой - мол у нас праздник/юбилей/распродаже и т.д., мы хотим вам подарить бонус/скидку/подарок. Чтобы активировать предложение - отправьте SMS вот с этим текстом на такой-то номер и будет вам счастье. Если это сделать по уму, то сумма, даже при получении всего лишь части от стоимости премиум-SMS может зашкаливать за сотни тысяч рублей за пару дней. Правда, для этого надо "простимулировать" нужных людей в операторе связи и контент-провайдере.

Еще один вариант - все акции, когда оператор готов доплачивать за входящие звонки свыше какого-то времени разговора или просто за сам факт такого вызова и разговора минуту или около того. Вот здесь включаются безлимитные номера и небольшие аппаратно-программные комплексы, которые совершают вызовы на заранее приобретенные номера такого "щедрого" оператора связи в постоянном режиме. Так "накачиваются" балансы весьма оперативно - потом либо "обнал" либо мобильный перевод для "обналички". Так "попали" в Tele2, были примеры и у "МегаФон".

Кстати, здесь четко прослеживается связь преступных группировок и сотрудников операторов связи. «СБ еще и контрразведкой надо заниматься, - отмечаю наши собеседники. - Наиболее "коррупционные" места все те, кто готовит документы для выплаты денег партнерам. Помню, поймали мы как-то за руку своего сотрудника, который занижал объемы фродовых контентных смс (тех, за которые денег не получить) и соответственно контент-провайдер получал куда как больше денег. Аналогичные проблемы были по дилерскому фроду - пустые договоры, липовые паспорта, но дилерскую комиссию получают. Кроме того, ловили и людей, которые без оснований подключали роуминг тем или иным "проблемным" SIM-картам, увеличивали кредитные лимиты без четких оснований для попадания "в минус" на pre-paid тарифам для отправки премиум SMS и т.д.»

Мошенники работают и с другими схемами «обнала» нечестно заработанных денег. Причем, сервисы операторов мобильной связи здесь используются не по прямому назначению. Наибольшее число фродовых атак реализуется в тех сервисах, где есть возможность вывести деньги любым относительно легким способом. К примеру, самый простой вариант подобных систем - купить номер мобильной связи на "левые" данные и пополнить его с карточки, данные которой были украдены. Разумеется, пользоваться таким номером сам злоумышленник не будет (хотя, случаются и такие варианты), но продать ее на вещевом рынке местным продавцам или криминальным элементам вполне возможно. С дисконтом, конечно, но это живые деньги.

Еще вариант - регистрируется какой-либо небольшой проект по продаже любой информации за премиальные SMS, туда нагоняется легальный трафик, под прикрытием которого с SIM-карт, оформленных на "левые" данные, отправляется туча платных SMS. Вывод денег в WebMoney чаще всего организуется. Но, конечно, живут такие проекты недолго, поскольку пополняют эти электронные счета мобильных телефонов с ворованных карт иностранных банков.

Не остаются без внимания и online игры. Здесь, в отличие от той же мобильной связи, полная анонимность - сложно выявить действия конкретного картхолдера и его аккаунты: есть только персонажи со своими никами и историей игры. Деньги на счет загоняют за оплаты игровой валюты и покупки артефактов, снаряжения и оружия, с помощью которой можно "прокачивать" свои персонажи. Несмотря на запрет продажи персонажей, практически во всех играх серый и черный рынок такого рода существует.