ФРОД И АНТИФРОД: практика операторов

Л.Павлова

DOI: 10.22184/2070-8963.2018.70.1.70.71

В цифровых реалиях вопросы борьбы с мошенничеством на сетях связи становятся все более актуальными для операторов. Какие рецепты антифрода они используют?

"Параллельный бизнес"

Для операторов связи фрод (от англ. fraud, мошенничество) – это нежелательный трафик, в основном телефонный. По статистике, операторы теряют до 5% выручки из-за мошеннических действий третьих лиц, когда через взломанное клиентское оборудование в короткий промежуток времени проходит большое количество сессий дальней связи. По экспертной оценке "МФИ Софт", ежегодные объемы потерь мобильных операторов РФ от незаконной терминации международного трафика составляют от 300 до 500 млн минут (порядка 3 млрд руб.); потери МГ/МН-операторов при завершении международного трафика на фиксированных сетях составляют от 200 до 300 млн минут (около 200 млн руб). А ежегодные объемы потерь зоновых и МГ/МН-операторов РФ от нарушений порядка пропуска междугородного трафика составляют до 2 млрд минут или от 2 до 3 млрд руб. Операторы предпринимают немалые усилия для борьбы с фродом, однако он эволюционирует (голосовая связь стремительно утекает в VoIP и OTT-сети, такие как Viber, Skype, WhatsApp) – и требует неослабевающего внимания со стороны компаний, несущих потери.

Как заметила в своем выступлении на 8-й Всероссийской конференции Revenue Assurance, Fraud, InfoSecurity & Risk Management Елена Асланова, начальник отдела по управлению фродом компании "ВымпелКом", нелегальная терминация трафика – это, по сути, параллельный бизнес, который существует вместе с операторским. Мошенники используют шлюзы, подключенные, с одной стороны, к сети Интернет и бирже VoIP-трафика, а с другой – к сети оператора по договору оказания услуг местной связи с безлимитным тарифом. Чтобы пресекать их деятельность, оператор использует системы автоматического выявления и распознавания нежелательного трафика, а также новые подходы к работе с каналами сбыта. "Последнее, что мы сделали, – научились блокировать заготовки, то есть SIM-карты до того как с них пошел трафик, до того как они попали в шлюзы, – рассказала Е.Асланова. – В тот момент, когда эти блокировки были внедрены, объем нелегальной терминации радикально упал. Но сейчас мошенники изменили свои алгоритмы – подмешивают входящий трафик, СМС-трафик, используют различные закольцованные схемы. В ответ мы запускаем новые правила для того, чтобы таких мошенников выявлять".

"ВымпелКом" предоставляет и услуги фиксированной связи. Для контроля фрода компания использует промышленное решение, дифференцированную систему порогов в зависимости от степени риска с выявлением фрода в режиме, близком к режиму реального времени. Задержка получается небольшая, но, по признанию Е.Аслановой, она пока не позволяет предоставлять услугу защиты от фрода в том виде, как ее ожидает рынок, поскольку иногда за полчаса "сливаются" порядка нескольких тысяч минут фродовского трафика. Проблема есть, и над ней компания сейчас работает.

Вместе – сильнее

Противодействие мошенничеству и гарантирование доходов (FM&RA) – достаточно зрелое в структуре крупных операторов направление, в функции которого входят: оценка рисков; построение системы контроля рисков; контроль рисков; проведение мероприятий по предотвращению и фиксации потерь. Эксперты "МФИ Софт" выделяют две

категории мер, принимаемых российскими операторами для защиты от фрода: превентивные (мероприятия, направленные на уменьшение количества фрода и закладывающие юридическую базу фиксации и устранения таких нарушений) и меры, фиксирующие и останавливающие факты фрода.

Кроме того, в последнее время наметилась тенденция объединения усилий крупнейших операторов в борьбе с фродом. Эти меры включают в себя как процедуры обмена информацией о фактах нарушений, так и использование ряда технических средств, автоматизирующих подобные процедуры. Такого рода взаимодействие позволяет не только ускорить поиск и ограничение реальных источников фрод-трафика, но и сократить общие потери операторов. Как отметил Алексей Кулешов, заместитель начальника отдела управления проектами ПАО "Ростелеком", только совместными усилиями с объединением всех антифродовских служб владельцев емкости можно решить задачу борьбы с фродом, причем с использованием системы для обмена данными по всем выявленным кейсам на некой единой платформе.

Так, в "Ростелекоме" реализована система аналитической отчетности на базе интерконнекта, ежемесячно обрабатывающая около 10 млрд записей. Аналитическое хранилище позволяет сократить время на подготовку отчетности, облегчает процесс бюджетирования, помогает оптимизировать тарифную политику для международных вызовов и, как следствие, повышает эффективность работы "Ростелекома" с операторами связи. Данные межоператорских расчетов разделены на сегменты в соответствии с типом номера абонента (B2O, B2B, B2C), что позволяет точно оценить маржинальность услуг по каждому из сегментов. "Мы получили инструмент, который позволяет нам оптимизировать тарифную политику, – пояснил А.Кулешов. – Теперь надо постараться абонентов других операторов переключить на свою сеть – и решать задачи внешней монетизации". Эта задача, по словам А.Кулешова, уже успешно решается благодаря недавно запущенному совместно с Tele2 проекту. Не приводя конкретных цифр, представитель "Ростелекома" подчеркнул, что буквально за два месяца с момента старта проекта достигнут синергический эффект: была собрана экспертиза специалистов обеих компаний и удалось заметно поднять стоимость международных вызовов.

В других вертикалях

Как показало международное исследование EY в области информационной безопасности "Кибербезопасность на новом витке: готовимся противостоять киберугрозам" за 2017 год, в котором приняли участие 1200 респондентов из более чем 20 секторов экономики разных стран, подавляющее число российских компаний полагают, что их служба кибербезопасности не в полной мере соответствует потребностям организации. Такого мнения придерживаются 98% респондентов. Согласно данным исследования 2016 года, ранее такого мнения придерживались 86% опрошенных. 71% отмечают необходимость увеличения бюджета на кибербезопасность до 50%; 77% респондентов видят в сотрудниках наиболее вероятный источник киберугрозы; 69% опрошенных не имеют специальной программы по сбору и анализу информации о киберугрозах или ограничиваются неформальными мероприятиями.

В исследовании отмечается, что растущая конвергенция, бурное развитие Интернета вещей, расширение цифрового ландшафта способствуют созданию благоприятной почвы для хакеров. В сложившейся ситуации бизнесу необходимо оценить свою устойчивость к следующим видам угроз: обычные атаки со стороны "простых" хакеров, которые пытаются взломать систему защиты с помощью бесплатных хакерских утилит, зная об уязвимостях этой системы; сложные атаки со стороны умелых злоумышленников, знающих о критических точках уязвимости в системе и использующих передовые технические средства; новые атаки со стороны технически подкованных хакеров с использованием новых технологий.

Респонденты отметили возрастание таких угроз кибербезопасности, как фишинг и вредоносное программное обеспечение: говоря об актуальных для бизнеса угрозах, 64% респондентов назвали их главными (в прошлом году такого мнения придерживались 52% и 51% соответственно). Что касается существующих уязвимостей, большинство респондентов (60%) видят их в неосмотрительности и неосведомленности сотрудников. Второе место заняли устаревшие средства контроля или архитектура безопасности (46% считают этот фактор актуальным для своего бизнеса), на третьем месте – несанкционированный доступ (37%).

По данным исследования, российские компании отстают от зарубежных по уровню зрелости процессов управления кибербезопасностью и их интеграции с бизнес-процессами, что усиливается общим несоответствием технического обеспечения информационной безопасности потребностям организации. ■