СМС-таргетинг для получения информации о клиентах. Внешние угрозы ИБ. Схема и методы противодействия.

Докладчик: Богданов Денис Викторович

Руководитель Отдела информационной безопасности

ООО МФК «ВЭББАНКИР»

Кейс: клиенту приходят SMS со ссылками на конкурентов и агрегаторов

Цели:

- определить используемый для утечки информации контур (внешний или внутренний) и фактический источник(-ки) утечки;
- определить схему SMS-рассылок конкурентами;
- предложить варианты решения, либо минимизации потерь.

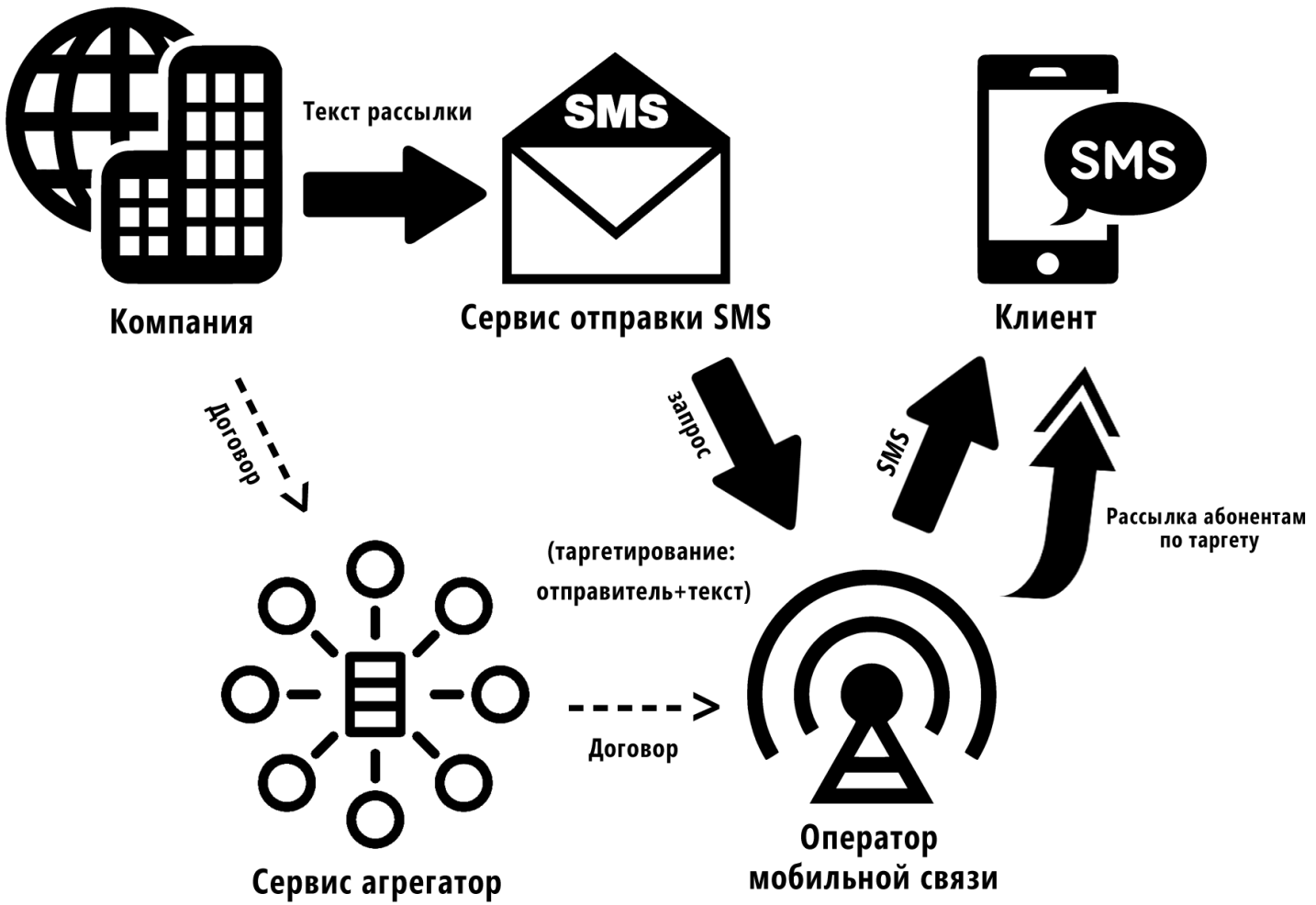
Исходные данные для теста:

- 3 номера телефонов (отсутствуют в базе компании), в сервис никогда не обращались, принадлежат трём разным операторам связи;

- отправка sms «руками», через тот же внешний сервис, откуда инициируется автоматическая рассылка клиентам;

- на каждый номер направлялись разные тексты (каждый следующий дополнял предыдущий), для определения таргета срабатывания;

- аналогичный текст был направлен с обычного номера телефона на 4-ый номер (для проверки того, что таргет срабатывает только на конкретного отправителя.


Текст рассылки
SMS
SMS
Компания
Сервис отправки SMS
Клиент
Договор
запрос
SMS
Рассылка абонентам
по таргету
(таргетирование:
отправитель+текст)
Договор
Сервис агрегатор
Оператор
мобильной связи

Почему эта ситуация актуальна?

Основные проблемы для организации:

- угроза безопасности данных клиента (части данных);
- уменьшение конверсии обращений клиентов к сервису;
- порча репутации перед клиентами;
- снижение прибыли.

Рекомендации по итогам расследования:

- использовать для информирования части клиентов (например, делающих заявку через app-приложение) отправку текста не через SMS, а через push-уведомления в приложении;

- изменение текста SMS (латиница), чтобы уменьшить вероятность срабатывания триггера (временная мера, но может помочь);

- замена Сервиса отправки SMS на другую (также временная мера);

- обсудить вопрос с агрегаторами лично, юридическая претензия.

Спасибо за внимание!