МТС на шаг впереди

«Защита абонентов связи от современных угроз»

Сергей Прадедов
заместитель вице-президента по безопасности
директор департамента информационной безопасности
ОАО “Мобильные ТелеСистемы”

МТС на шаг впереди

СОДЕРЖАНИЕ

Обзор презентации

- **Предпосылки развития фрода на сетях связи**
- **Распространенные виды фрода в отношении абонентов**
- **Направления работы:**
  - Противодействие фроду на контент-услугах
  - Борьба с SMS-спамом
  - Защита от вирусов для мобильных устройств
  - Борьба с мошенничеством с подменой А-номера
  - Услуги безопасности для абонентов
  - Повышение грамотности абонентов в области ИБ
- **Заключение**

ПРЕДПОСЫЛКИ РАЗВИТИЯ ФРОДА

Направленные атаки

Рост атак коммерческих организации под заказ

Рост мобильных угроз

Мобильные платформы все более привлекательны для кибер-преступности:

- Рост числа смартфонов.
- Расширение сервисов для смартфонов.
- Развитие мобильного Интернета.
- Рост производительности смартфонов.
- Перевод электронных кошельков и интернет-банкингов на смартфоны.

Готовые наборы для атак

Готовые наборы для атак, позволяющие взламывать системы не обладая специальными знаниями, получили все большее развитие

Развитие соц. сетей

Развитие соц. сетей существенно упростило злоумышленникам задачу поиска информации о цели атаки

Сокрытие своих следов

Все чаще злоумышленники скрывают свои следы, а не афишируют факты своих взломов

НАИБОЛЕЕ РАСПРОСТРАНЕННЫЕ ВИДЫ ФРОДА В ОТНОШЕНИИ АБОНЕНТОВ

- Мошенническое и вирусное ПО для мобильных устройств
- Мошенничество при предоставлении контент-услуг
- SMS-спам рассылки мошеннического характера
- Звонки и SMS-сообщения с подменой номера с целью мошеннических действий
- Взлом абонентских кабинетов платежных систем с целью вывода финансовых средств
- Взлом личных кабинетов абонентов с целью мошеннических действий
- Взлом абонентского оборудования фиксированной сети и генерация трафика на международные направления или платные сервисы
- Звонковый DoS для отказа абонентом от использования своего номера
- Социальная инженерия

ПРОТИВОДЕЙСТВИЕ ФРОДУ НА КОНТЕНТ-УСЛУГАХ

Для защиты абонентов от мошенничества при использовании контентных услуг реализован целый комплекс мер:

- внедрена система обязательного информирования абонентов о стоимости контент-подписок
- организовано взаимодействие с «Яндексом» по выявлению популярных интернет ресурсов, рекламирующих и предоставляющих мошеннические контентные услуги
- создан специальный центр мониторинга и тестирования контент-услуг
- организовано взаимодействие с «Лабораторией Касперского» по выявлению мошеннического ПО для мобильных устройств для подключения абонентам контент-услуг
- пересмотрены отношения с контент-провайдерами и кратно повышены для них штрафы за нарушения условий продажи контента

ЗАЩИТА АБОНЕНТОВ ОТ SMS-СПАМА

Внутрисетевой спам:

- внедрена автоматизированная система «Антиспам»
- Услуги SMS Pro и «Черный список» и короткий номер 1911 для абонентов
- Объем мошеннического SMS-спама в 2013 году снизился в 20 раз

Массовые рассылки из внешних сетей:

- Перевод трафика рекламно-информационного характера на прямые договоры с распространителями с июля 2013 года
- Блокировка спама с коротких и буквенно-символьных номеров в декабре 2013 года

Первые итоги:

- Число SMS из внешних сетей с признаками спама сократилось в пять раз – до 200 млн в декабре 2013 года по сравнению с 950 млн в ноябре
- Количество жалоб абонентов на спам и мошенничество в декабре сократилось в 4,5 раза

В декабре 2013 года в Госдуму внесен законопроект «О внесении изменений в ФЗ«О связи» (в части регулирования рассылок по сети подвижной радиотелефонной связи)», автор Р. Гаттаров, который вводит определение рассылок, предусматривает заключение прямого договора с распространителем, обязывает заказчика рассылки доказывать наличие согласия абонента на ее получение, а также позволяет абоненту отказаться от рассылки, обратившись напрямую к оператору.

ЗАЩИТА ОТ ВИРУСОВ ДЛЯ МОБИЛЬНЫХ УСТРОЙСТВ

Проблема:

- Абоненты России входят в лидеры по угрозе заражения своих смартфонов (по данным «Лаборатории Касперского» – второе место в мире, по данным Lookout - первое).
- Более 50% от всех экземпляров мошеннического ПО для мобильных устройств, выявляемых в мире, разработано против абонентов российских операторов (Lookout, Def Con USA 2013)
- Самый распространённый вид мошеннического ПО для мобильных устройств - ПО, которое скрытно осуществляет рассылку смс-сообщений на короткие-платные подписочные номера.

Меры по защите абонентов на примере сотрудничества с KASPERSKY lab

- Взаимодействие с «Лабораторией Касперского» включает в себя:
  - ежедневные отчеты о новых вирусах для мобильных устройств
  - анализ вирусов для мобильных устройств, выявленных на основании жалоб абонентов МТС и информации оборудования сети связи
  - Выявление новых способов вывода средств с лицевых счетов абонентов, которые используются вирусами для мобильных устройств
- Организована блокировка вирусов и вредоносных сайтов с целью минимизации ущерба наносимого абонентам

В 2013 году:

Выявлено более 350 новых вредоносных программ

Заблокирован доступ к более чем 7 тыс. ссылкам на вирусное и мошенническое ПО

Предотвращено более 700 тыс. попыток переходов абонентов МТС по мошенническим ссылкам

Заблокировано 38 центров управления бот-сетей

ЗВОНКИ МОШЕННИЧЕСКОГО СОДЕРЖАНИЯ И ЗВОНКОВЫЙ DOS С ПОДМЕНОЙ А-НОМЕРА

Описание проблемы:

- Недобросовестные операторы при маршрутизации МГ/МН звонка могут осуществлять подмену вызывающего номера А-номера на местный номер при приземлении звонка на сеть другого оператора. Подобный звонок воспринимается принимающим оператором и его абонентом как местный.
- Ежегодно крупный оператор фиксирует более 10 тысяч случаев организации звонков, пришедших из сетей связи сторонних операторов на абонентов с подменой А-номера
- Злоумышленники могут использовать подмену А-номера для противоправных действий: звонковые DOS-атаки, спам, мошенничество
- Техническая простота организации подмены А-номера, распространённость VoIP-сетей делают данный вид фрода на сетях связи все более распространённым явлением.
- Существующая нормативно-правовая база РФ в отрасли связь не регламентирует требований к операторам в части подмены А-номера
- **Негативные последствия подмены А-номера для абонента:**

- ухудшение качества связи вплоть до обрыва звонка
- невозможность идентификации вызывающего абонента, недостоверная детализация звонков
- угроза безопасности государства и граждан
- возможность доступа третьих лиц к телефонным переговорам
- совершение мошеннических и противоправных действий в отношении абонента

Принимаемые операторами меры:

- Мониторинг сетевых стыков со сторонними операторами связи с целью выявления звонковых DOS и расследования инцидентов подмены номера А.
- Тестовые звонки по МГ/МН направлениям с целью выявления инцидентов подмены номера А

В январе 2014 года депутатами Я.Ниловым и И.Лебедевым в Госдуму внесен законопроект о внесении изменений в статью 46 федерального закона «О связи». Поправки обязывают оператора передавать информацию о номере вызывающего абонента без изменений, то есть запрещают подмену А-номера.

Черный список и SMS Pro

«Черный список» предоставляет возможность блокировки нежелательных входящих звонков и sms сообщений. Вы сами заносите номера нежелательных и желательных абонентов в список услуги и решаете, может ли этот абонент дозвониться до вас или нет.

Антивирус

«Антивирус» – это комплексная и простая в использовании on-line защита от шпионских программ, троянов, вирусов, червей, кражи паролей и других кибер-угроз. Для работы услуги не нужны специальные настройки или загрузка обновления антивирусных баз.

Родительский контроль

«Родительский контроль» - позволяет защитить ребенка от нежелательной информации при использовании мобильного Интернета от МТС. Данная услуга ограничивает доступ к веб-страницам, содержащим информацию для взрослых, азартные игры, нецензурную лексику, экстремистские, пропагандирующие насилие или наркотики материалы – всего свыше 80 категорий опасного контента. Для работы услуги не нужны специальные настройки или загрузка дополнительного программного обеспечения, при активированной услуге не загружаются ресурсы мобильного устройства или компьютера.

ПОВЫШЕНИЕ ОСВЕДОМЛЁННОСТИ АБОНЕНТОВ В ОБЛАСТИ ЗАЩИТЫ ОТ МОШЕННИЧЕСТВА - SAFETY.MTS.RU

МТС на шаг впереди

На основной сайт МТС

Безопасность — это просто

Предупреждён — значит вооружён!

Интернет | Мобильная связь | Фиксированная связь | Банковская карта | Дети в Интернете | Борьба с мошенничеством

„Дети в Интернете"

Простые уроки и правила полезного и безопасного Интернета для детей и взрослых

Подробнее

Пострадали от мошенников?

- Позвоните 8 800 250 0890
- Напишите на 911@mts.ru

- Хотите отписаться от рассылок?
  Наберите *111*919#
- Хотите узнать стоимость отправки SMS/MMS или звонка на короткий номер?
  Введите короткий номер:

Найти

БЕЗОПАСНАЯ МОБИЛЬНАЯ СВЯЗЬ

Соблюдайте простые правила, чтобы защититься от мошенников.

Подробнее

БЕЗОПАСНЫЙ ИНТЕРНЕТ

Соблюдайте меры безопасности при работе во всемирной сети.

Подробнее

УСЛУГА «ЧЕРНЫЙ СПИСОК»

Управляйте своим кругом общения!

*111*442#

Подробнее

ЗАКЛЮЧЕНИЕ

Для защиты абонентов от киберугроз в современных условиях необходимо:

- Скоординированная работа всех подразделений компании , задействованных в борьбе с фродом

  необходима интеграции систем противодействия фроду, классических систем мониторинга информационной безопасности и защиты IT-инфрастуктуры и систем мониторинга технических служб, эксплуатирующих сеть

- Сотрудничество с другими участниками рынка: операторами связи, банками, интерне-компаниями и прочими организациями

- Повышение грамотности абонентов в вопросах информационной безопасности при использовании телекоммуникационных и финансовых услуг

- Подготовка кадров, задействованных в борьбе с фродом

МТС на шаг впереди

Вопросы ?

Сергей Прадедов sap@mts.ru

заместитель вице-президента по безопасности
директор департамента информационной безопасности
ОАО “Мобильные ТелеСистемы”