МТС на шаг впереди

Противодействие фроду, направленному на клиентов финансово-кредитных учреждений

Ермаков Алексей
департамент информационной безопасности
ОАО “МТС”

МТС на шаг впереди

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. стей существенно упростило злоумышленникам задачу поиска информации о цели атаки

Сокрытие своих следов

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

МТС на шаг впереди

ОСНОВНЫЕ ФАКТОРЫ, ВЛИЯЮЩИЕ НА РАЗВИТИЕ ФРОДА

Факторы	Риски
Консолидация и централизация инфраструктуры • Органический рост • Внедрение новых технологий	■ Новые виды угроз ■ Ошибки и уязвимости в сложных системах и технологиях ■ Увеличение рисков ИБ
Повышение эффективности бизнеса • Интеграция компаний • Снижение издержек • Сокращение персонала	■ Приобретение и интеграция с компаниями с низким уровнем зрелости процессов ИБ и противодействия фроду ■ Снижение общего уровня защищённости ■ Снижение лояльности персонала
Взрывной рост киберугроз и изменение ориентиров киберпреступности • Киберпреступность трансформировалась в высокоорганизованную отрасль теневого бизнеса • Несовершенство законодательной базы по противодействию киберпреступности. • Низкий уровень культуры ИБ и осведомленности населения • Рост ИТ-технологий (особенно мобильных), интернет-банкингов и моб.платежей • Смещение интереса преступников с нанесения ущерба корпорациям к клиентам этих корпораций	■ Рост прямого и косвенного ущерба от действий фродстеров у компании и абонентов ■ Рост сложности противодействия угрозам ■ Отсутствие адекватной поддержки со стороны правоохранительных органов ■ Возможность массовой манипуляции абонентами и нанесение им ущерба ■ Упрощение способов монетизации дохода преступных группировок

НЕСАНКЦИОНИРОВАННАЯ ЗАМЕНА SIM-КАРТЫ

Вектор атаки:

- Получение мошенниками SIM-карты с использованием поддельных документов;
- Кража одноразового пароля или совершения звонков, отправки/получения SMS сообщений от имени абонента.

Примеры других событий, при наступлении которых возникают риски кражи средств :

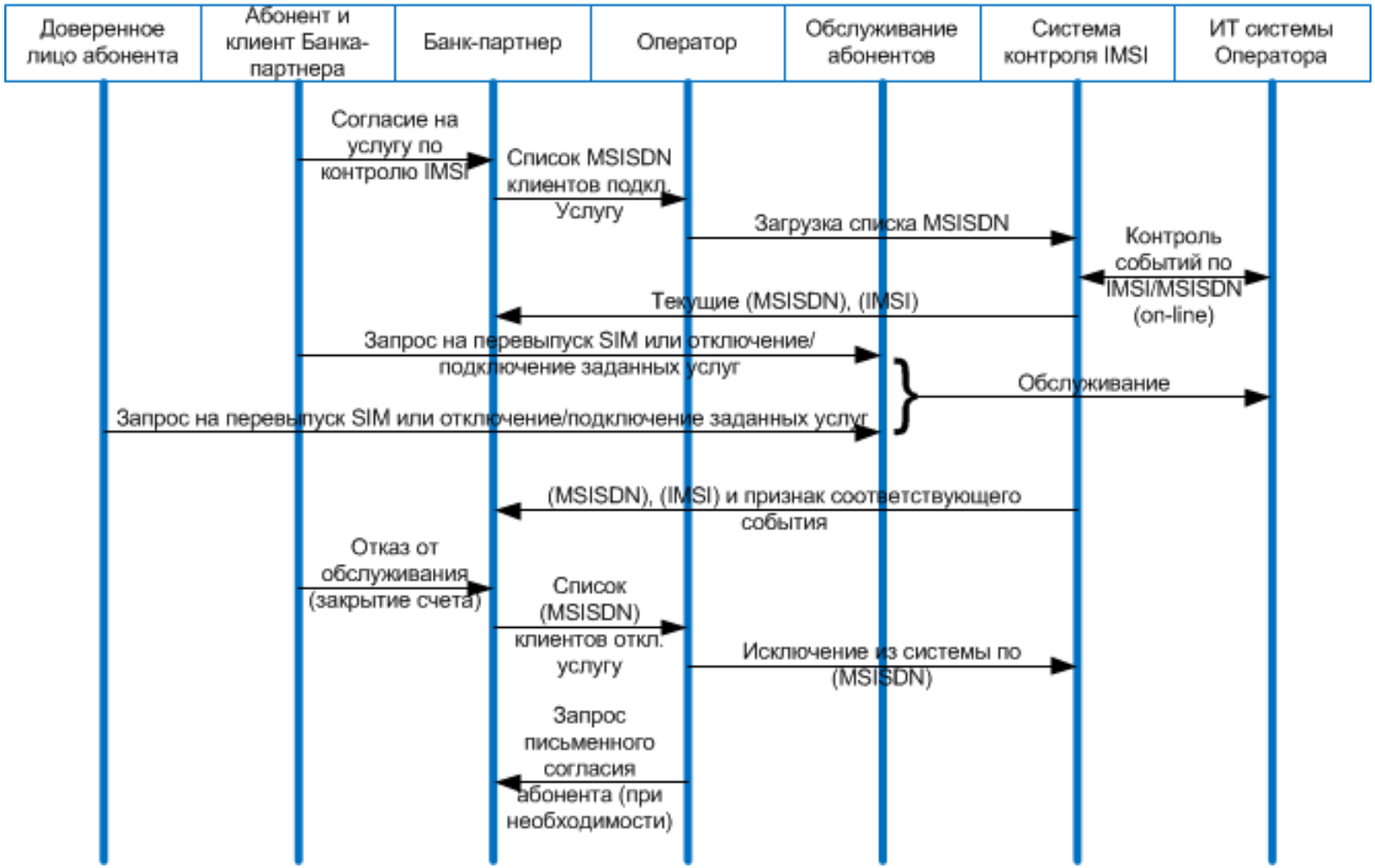
- Установка переадресации SMS сообщений с номера «жертвы» на телефон мошенников;
- Установка переадресации голосовых вызовов с номера «жертвы» на телефон мошенников;
- Блокировка телефона «жертвы»;
- Переход телефонного номера клиента, к которому была подключена услуга банковского SMS-информирования, в использование другому человеку, без отключения данной услуги;
- Переход телефонного аппарата, на котором было установлено приложение мобильного банкинга, в использование другому человеку, без удаления приложения;
- Расторжение абонентом контракта на обслуживание;

Принятые меры:

- Разработан сервис «Контроль событий обслуживания абонентов».

МТС на шаг впереди

ЛОГИКА РАБОТЫ СИСТЕМЫ КОНТРОЛЯ СОБЫТИЙ ОБСЛУЖИВАНИЯ АБОНЕНТОВ



МОШЕННИЧЕСКИЕ СМС РАССЫЛКИ

Вектор атаки:

– Преступники, обладающие приемами психологического влияния, вводят человека в заблуждение, убеждая совершить действия, которые приводят к компрометации его банковской карты, аккаунта сервиса ДБО или переводу средств на счет мошенников.

Предложение:

– Осуществлять on-line информирование банка, в котором обслуживается клиент, о поступлении абоненту SMS сообщения, классифицированного как «банковский фрод». Получение этой информации банком, обеспечивает возможность проактивной реакции на события, при наступлении которых возникает риск кражи средств у клиента банка.

Примеры мошеннических рассылок							
Количество отправленных сообщений	A-номер	Текст сообщения	Время начала отправки	Время окончания отправки	Правило антиспама	Процент уникальных b-номеров	Количество уникальных b-номеров
9 300	791********	ВАША БАНКОВСКАЯ КАРТА VISA ЗАБЛОКИРОВАНА Инфо:9:00 22:00 +79512701394	03.02.2013 1:00:24	03.02.2013 1:10:51	1	100	9 300
279	790********	Ваша карта VISA заблокирована. Горячая линия 8-800-555-30-87 ЦБ РОССИИ	02.02.2013 10:17:17	02.02.2013 11:22:51	1	99	276

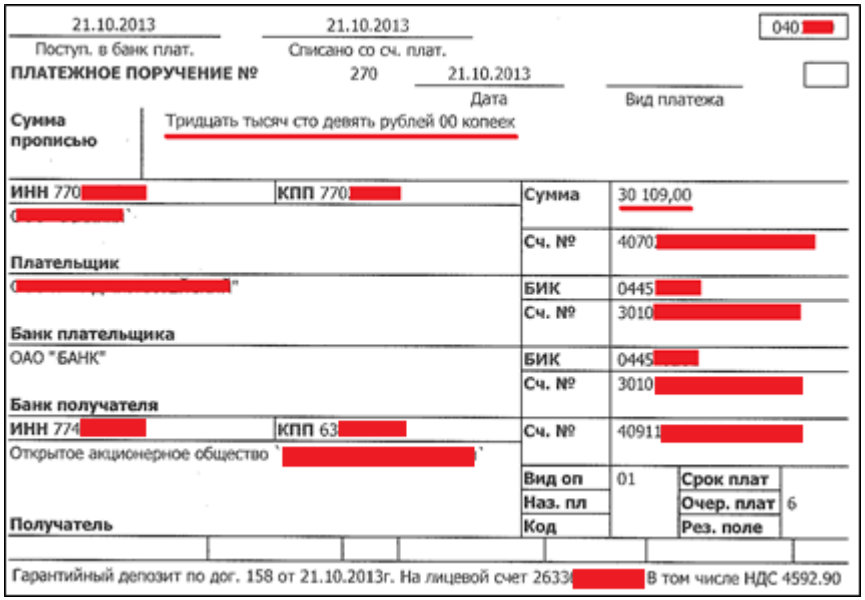
ИСПОЛЬЗОВАНИЕ ЛИЦЕВЫХ СЧЕТОВ АБОНЕНТОВ ДЛЯ ВЫВОДА ДЕНЕГ С БАНКОВСКИХ СЧЕТОВ ЧЕРЕЗ ДБО

Вектор атаки:

- Компроментация ДБО клиента третей организации с целью совершения несанкционированных платежей на лицевые счета абонентов и последующим выводом средств на электронный счет злоумышленников.
- Использование лицевого счета абонента в качестве транспорта средств.

Предложение:

- Выполнять предварительную on-line валидацию номера счета, на который осуществляется зачисление средств.
- Осуществлять автоматизированное информирование о ранее скомпрометированных телефонных номерах и лицевых счетах для инициирования расследования по ним.



21.10.2013 Поступ. в банк плат. | 21.10.2013 Списано со сч. плат. | 040[redacted]

ПЛАТЕЖНОЕ ПОРУЧЕНИЕ № 270 | 21.10.2013 Дата | Вид платежа

Сумма прописью: Тридцать тысяч сто девять рублей 00 копеек

ИНН 770[redacted]	КПП 770[redacted]	Сумма	30 109,00
[redacted]		Сч. №	4070[redacted]
Плательщик			
[redacted]		БИК	0445[redacted]
		Сч. №	3010[redacted]
Банк плательщика			
ОАО "БАНК"		БИК	0445[redacted]
		Сч. №	3010[redacted]
Банк получателя			
ИНН 774[redacted]	КПП 63[redacted]	Сч. №	40911[redacted]
Открытое акционерное общество [redacted]		Вид оп	01
		Наз. пл	
Получатель		Код	
		Срок плат	
		Очер. плат	6
		Рез. поле	

Гарантийный депозит по дог. 158 от 21.10.2013г. На лицевой счет 2633[redacted] В том числе НДС 4592.90

РАСПРОСТРАНЕНИЕ ВРЕДОНОСНОГО ПО

Предпосылки:

–Согласно отчёту компании Lookout, более 50% от всех экземпляров вредоносного ПО для мобильных устройств, разработано против абонентов российских операторов, а мобильные устройства абонентов России занимают первое место по угрозе заражения*.

–Основной целью злоумышленников являются мобильные устройства на базе ОС Android, так как в отличие от других ОС в этом случае абонент может производить установку приложений из не доверенных источников в обход официального магазина приложений.

–Распространение Botnet-сетей и рост количества зараженных мобильных устройств.

Вектор атаки:

–Загрузка вируса на Android устройство с целью получения удаленного контроля.

Базовый функционал вирусов:

–Кража паролей и параметров доступа к банковским сервисам.

–Вывод денежных средств с мобильных счетов абонентов.

–Копирование истории звонков и контактов из записной книжки.

–Кража SMS-переписки.

–Запись телефонных переговоров абонента.

–Удаленное управление мобильным устройством, в том числе удаленное включение микрофона.

–Определение местоположения абонента и передача координат.

–Использование зараженного мобильного устройства для организации DDoS атак и спам-рассылок.

* - Отчёт, представленный специалистами компании Lookout на конференции Def Con USA 2013: https://www.lookout.com/resources/reports/dragon-lady

РАСПРОСТРАНЕНИЕ ВРЕДОНОСНОГО ПО

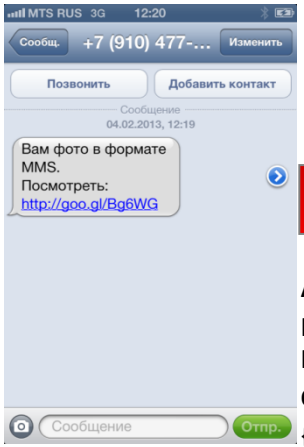
Принятые меры

- Предупреждение заражения мобильных устройств путем, блокировки источников распространения вредоносного ПО.
- Блокировка центров управления зараженными устройствами.

Предложение:

- Осуществлять информирование банков о событиях вероятного заражения абонентов.
- Осуществлять информирование банков о модели мобильного устройства.

1. Массовая рассылка.



2. Инфицирование и удаленное управление.

Адрес центра управления:

http://wap-look.com/download/file.php?id=354457053212100

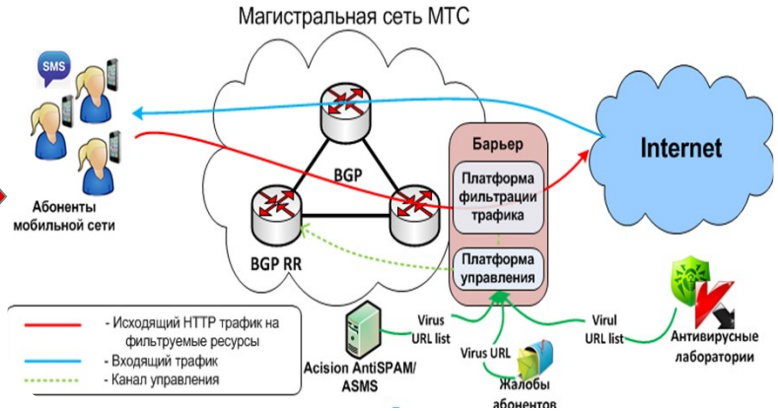
Ответ центра управления:

{"number":"*123*","text":"*9101234567* 1000", "time":"10", "aos":"1", "aos_text":"1","server":"wap-look.com"}

Содержание команды:

Отправить СМС на номер *123* с текстом "*9101234567* 1000", через 10 сек. отправить одно ответное сообщение с текстом "1", выбрать центром управления "wap-look.com".

3. Проактивные действия.



- Выполнить блокировку доступа к источнику распространения вредоносного ПО (предупреждение заражения).
- Выполнить блокировку доступа к центрам управления (нарушение работоспособности вируса).

МТС на шаг впереди

ОПЕРАТИВНОЕ ВЗАИМОДЕЙСТВИЕ

В целях оперативного реагирования на новые типы угроз и схемы фрода предлагается организовывать взаимодействие между ответственными подразделениями финансово-кредитных организаций и ответственными дежурными подразделениями операторов связи.

МТС

Для внутреннего использования

УТВЕРЖДЕН

Распоряжением от "__" _____ 201_ г. №_____

Рабочая инструкция
«Взаимодействие с коммерческими банками и организациями, оказывающими финансовые услуги в рамках реализации совместных мер противодействия мошенничеству»

Ответственный за применение НД:

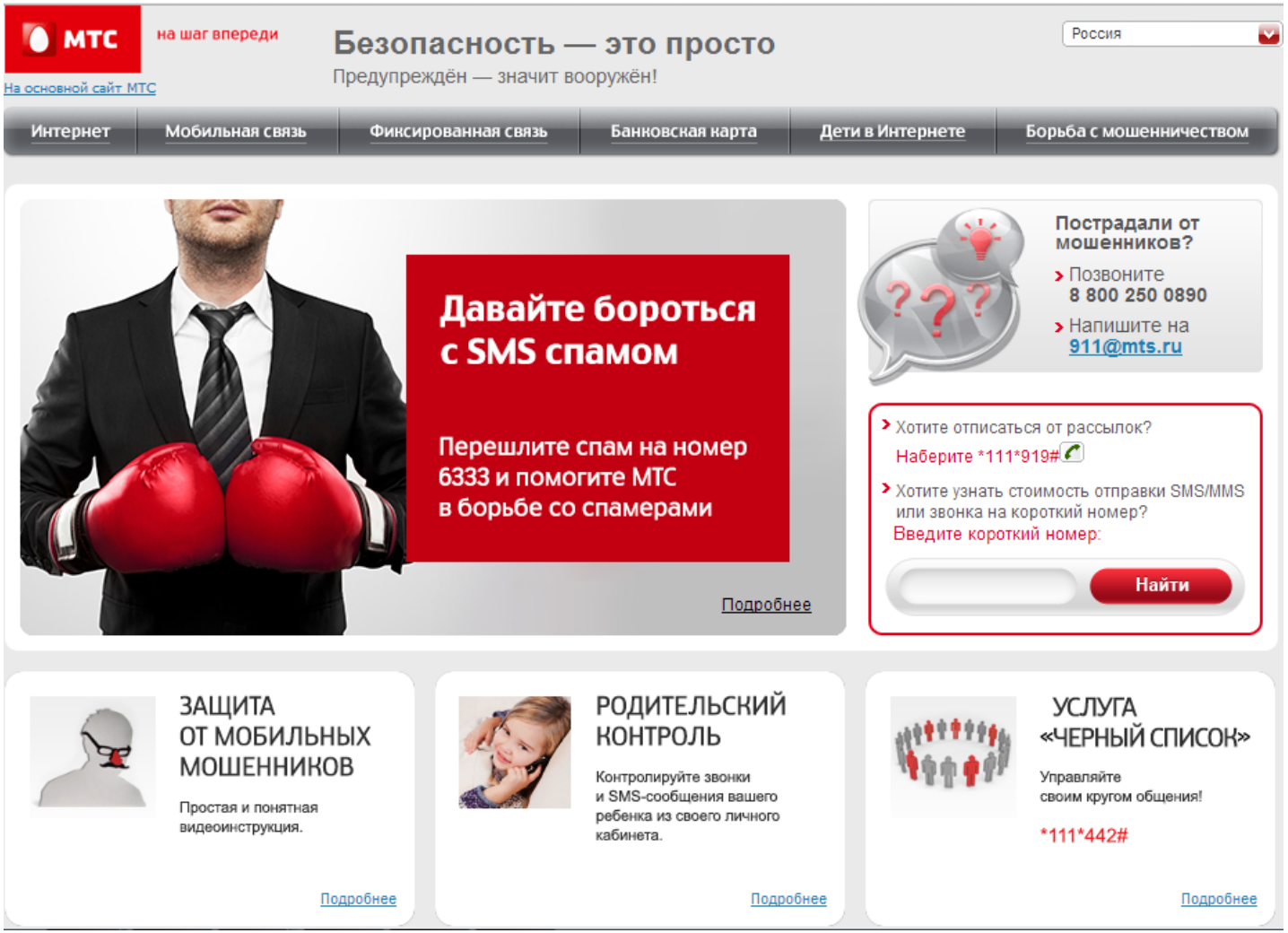
Корпоративный центр\Блок по безопасности\Департамент информационной безопасности\ Отдел противодействия фроду на сетях связи\ Начальник отдела

СБЕРБАНК

МТС Банк

МТС на шаг впереди

WWW.SAFETY.MTS.RU
ВСЕ ДЛЯ ПРЕДУПРЕЖДЕНИЯ И ЗАЩИТЫ АБОНЕНТОВ ОТ МОШЕННИЧЕСТВА



МТС на шаг впереди

Вопросы?

Ермаков Алексей
Email: avyerma2@mts.ru

департамент информационной безопасности
ОАО “МТС”