Расследование инцидентов, связанных с мобильными бот-сетями и вредоносным ПО

Николай Гончаров – **аспирант МГТУ им. Н.Э. Баумана, кафедра «Информационная безопасность»**
Денис Горчаков – **эксперт по расследованию инцидентов, коммерческий банк**

Вредоносное ПО для мобильных устройств

В связи с ростом числа пользователей смартфонов на базе OS Android основной угрозой фрода в отношении абонентов в 2014 году стало широкое распространение различных вредоносных приложений, позволяющих злоумышленникам осуществлять скрытый от абонентов несанкционированный вывод денежных средств с их лицевых счетов.

Как правило, зараженные устройства образуют бот-сети, благодаря чему злоумышленники имеют возможность управлять активностью и изменять конфигурацию ботов удаленно через центры управления бот-сетями.

Вредоносное ПО для мобильных устройств: Дополнительные функции

Во вредоносных приложениях зачастую присутствуют дополнительные функции, служащие для достижения следующих целей:

- **Затруднить самостоятельное удаление абонентом приложения с мобильного устройства.**
- **Сделать активность приложения похожей на собственноручные действия абонента, в том числе чтобы затруднить оперативное выявление со стороны оператора связи.**

Некоторые из таких функций:

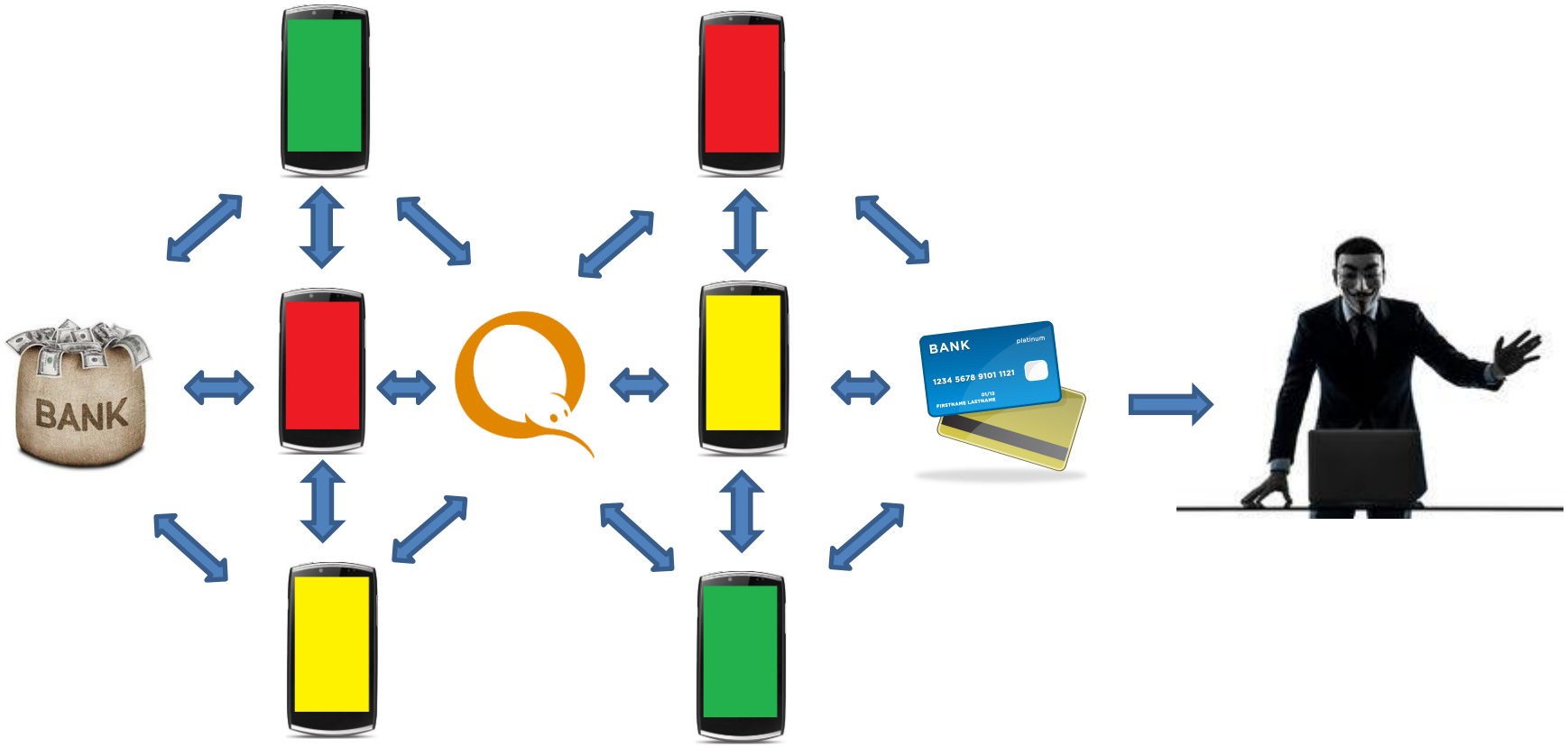
- **Отправка SMS-сообщений с произвольной задержкой по времени.**
- **Запрос привилегий «Администратора устройства» и даже root-прав доступа.**
- **Осуществление вредоносной активности в зависимости от местоположения абонента на основании Wi-Fi позиционирования, GPS и данных с базовых станций.**
- **Установка пароля на разблокировку экрана и стирание всех данных с внутренней памяти устройства после попытки удалить вредоносное приложение.**
- **Перехват информации о балансе лицевого счета абонента, что позволяет злоумышленникам заранее узнать, сколько денежных средств удастся вывести.**
- **Блокировка звонков на номера контактных центров операторов связи или переадресация таких звонков на другие номера.**

Угрозы бот-сетей

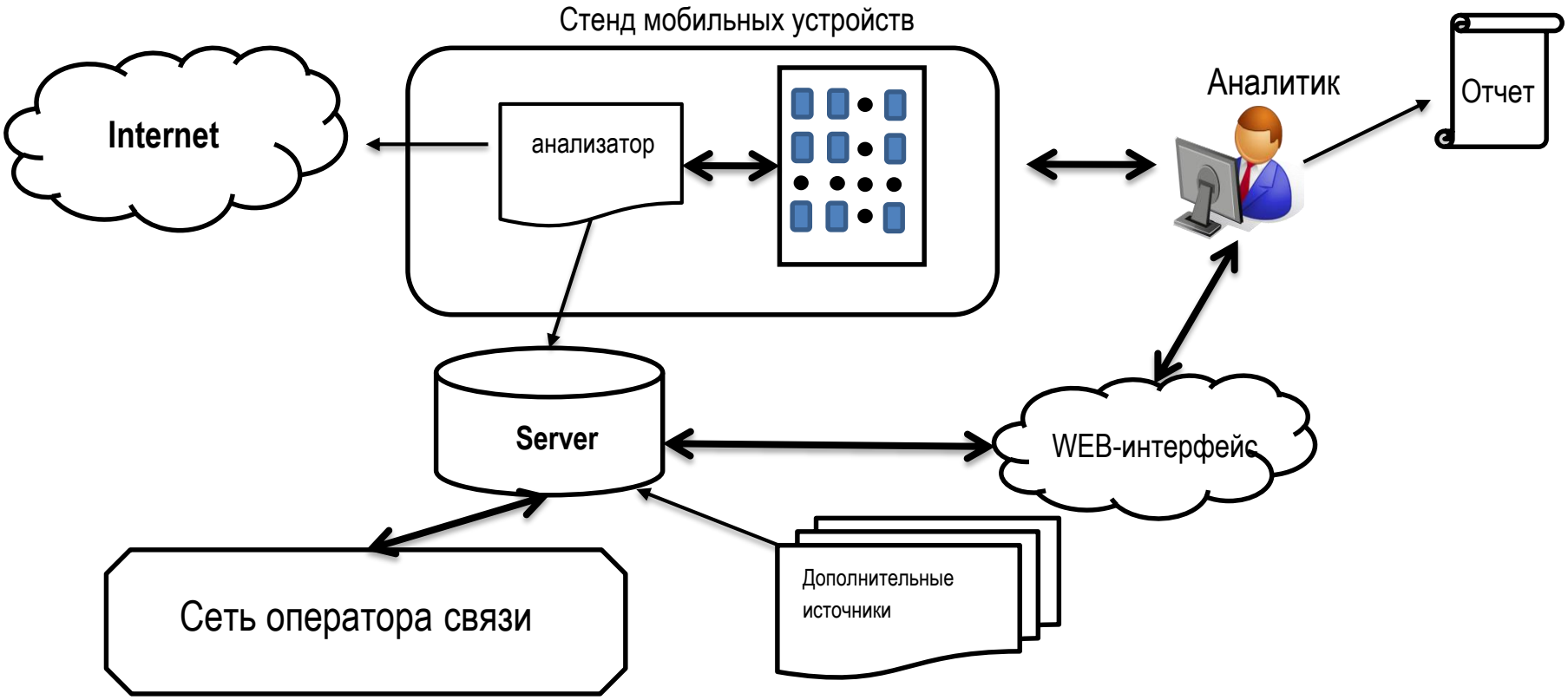
- Похищение персональных и конфиденциальных данных
- Рассылка спама
- Фишинг
- Анонимный доступ в сеть
- Кибершантаж и осуществление DDoS
- Получение сведений о местоположении конкретного человека
- Похищение денег, в том числе используя мобильную коммерцию и контент-услуги
- Влияние на работу различной техники и портативных устройств

Размытие границ ответственности

Высокотехнологичный фрод затрагивает всех участников рынка – в одну мошенническую цепочку попадают банки, платежные системы, операторы, что затрудняет расследование инцидентов.

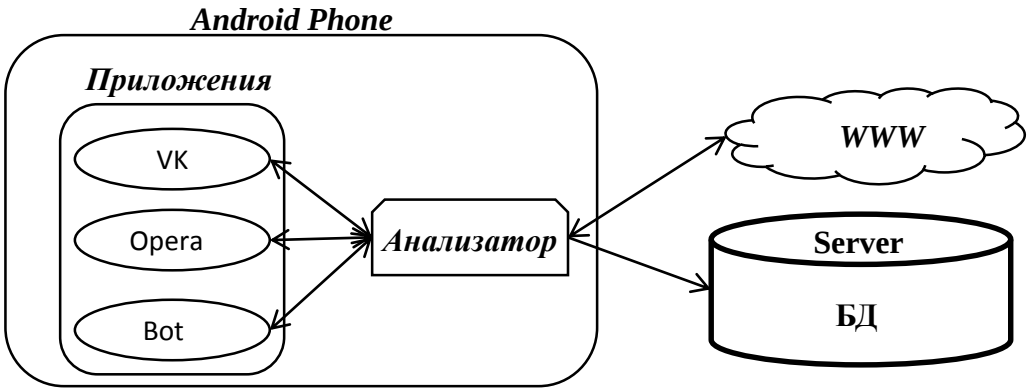


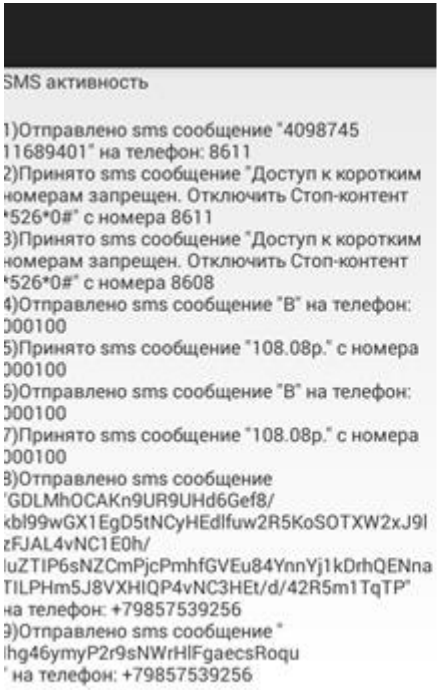
Комплекс по анализу приложений



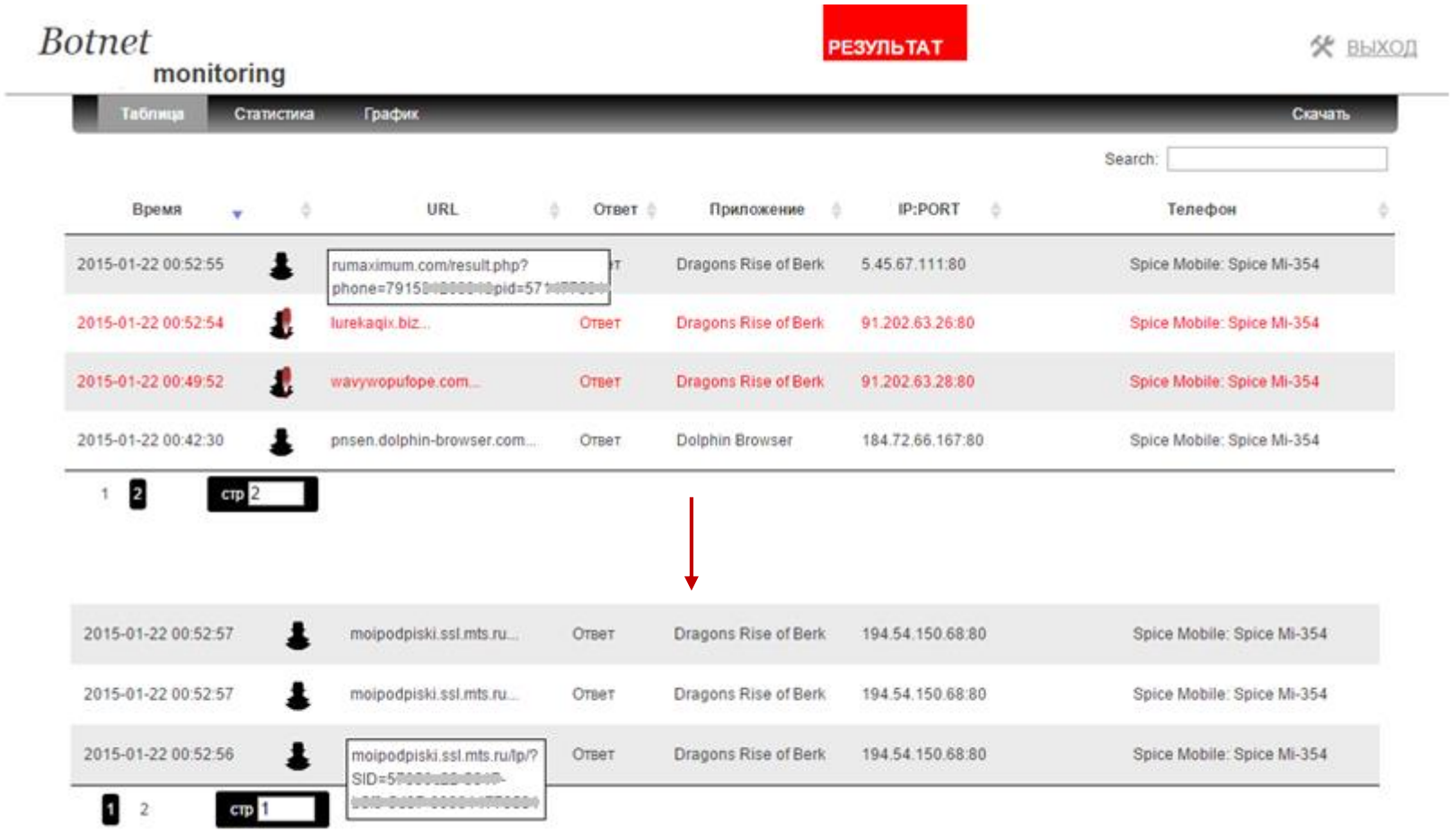
Данный комплекс обеспечивает динамический анализ и выявляет разнообразную активность бот-сетей.

Работа мобильного приложения

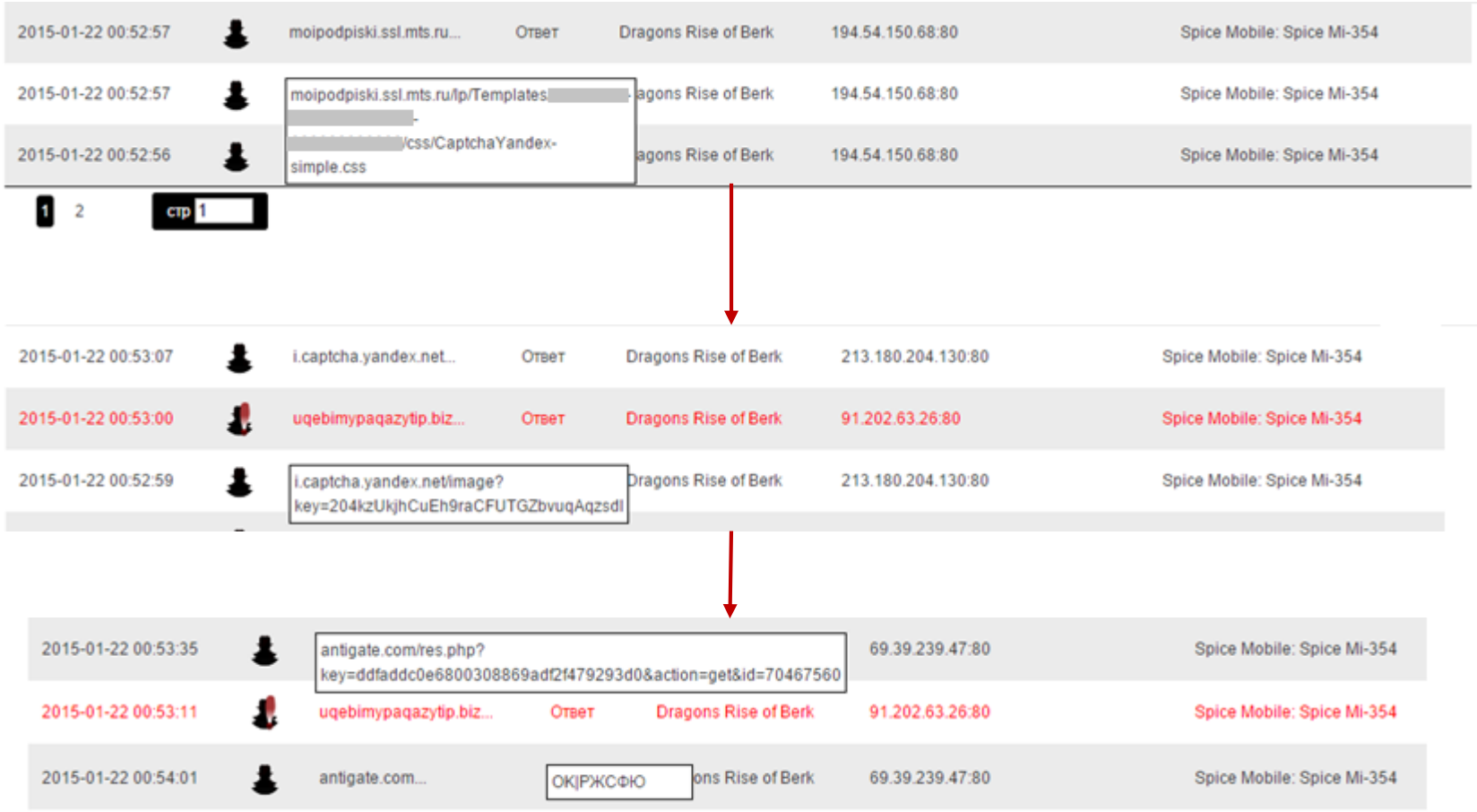




Web-интерфейс – пример инцидента



* - Подробное описание вредоноса: http://securelist.ru/analysis/obzor/25249/sms-troyanec-obxodit-captcha/



Всего запросов: 29

Таблица запросов:

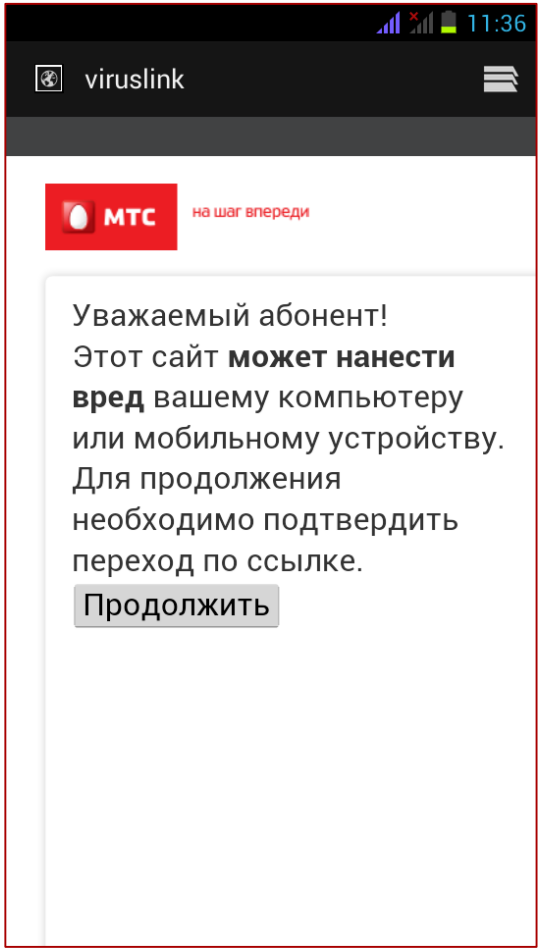
Dragons Rise of Berk	moipodpiski.ssl.mts.ru	8
Dragons Rise of Berk	rumaximum.com	7
Dragons Rise of Berk	uqebimypaqazytip.biz	4
Dragons Rise of Berk	antigate.com	3
Dragons Rise of Berk	i.captcha.yandex.net	2
Dragons Rise of Berk	lurekaqix.biz	1
Dragons Rise of Berk	api.sub.payments.tools	1
Dragons Rise of Berk	wavywopufope.com	1
Dragons Rise of Berk	cb.mts.sub.totmoney.ru	1
Dolphin Browser	pnsen.dolphin-browser.com	1

Схема работы решения

- Данная схема применима для информирования абонентов, а также для клиентов банков и финансовых организаций.

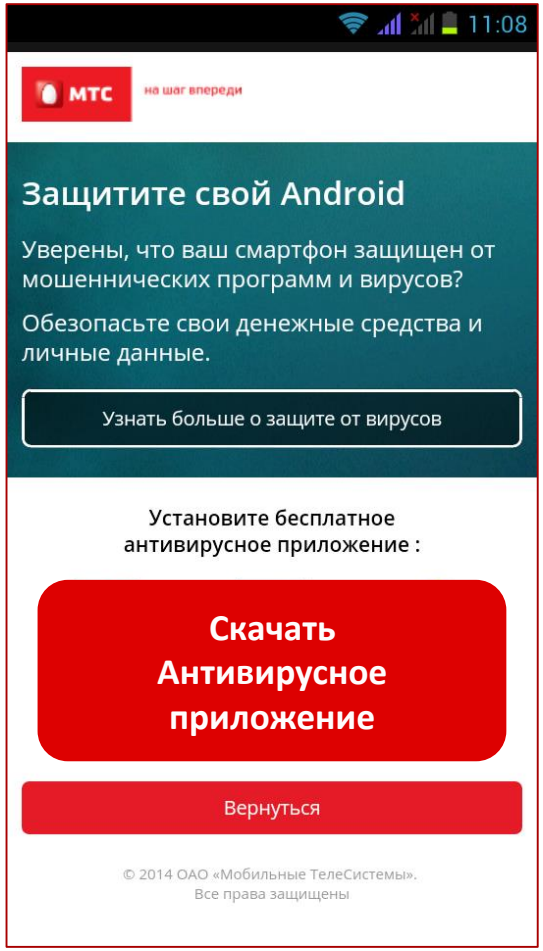
Меры противодействия по результатам расследования инцидентов

Предупреждение абонентов о сайтах, распространяющих вредоносное ПО для мобильных устройств, с использованием информационной WEB-страницы.



Информирование абонентов с рекомендациями по защите от фрода:

SMS рассылки, IVR-обзвоны и WEB-редирект для пользователей OS Android.



Обоснование реализации

Вы спрашивали после нашего доклада на ZeroNights 2014 – отвечаем:*

Недостаток антифрод-мониторинга на основе правил (пр. Intellinx):

- Нужно некоторое количество инцидентов для срабатывания правила.
- Мошенники постоянно "пробуют" лимиты правил, подбирая их экспериментальным путём.

Добавление нашего комплекса решает проблему и до срабатывания определённого количества правил, не зависит от установленных лимитов.

Недостатки статического метода по анализу кода вредоносного ПО:

- Неполнота получаемых данных ввиду использования множества динамических параметров, выполняемых в ходе работы приложения.
- Эффективные антиотладочные решения (см. предыдущие слайды).

Почему именно аппаратное решение?

- Сложность доработки и разработки существующих технических решений (эмуляторы, фреймворки) для борьбы с антиотладочными приёмами.
- Другая цель: сбор данных, а не взлом и реверс-инжиниринг приложения, мы ИБ, а не антивирусная лаборатория.

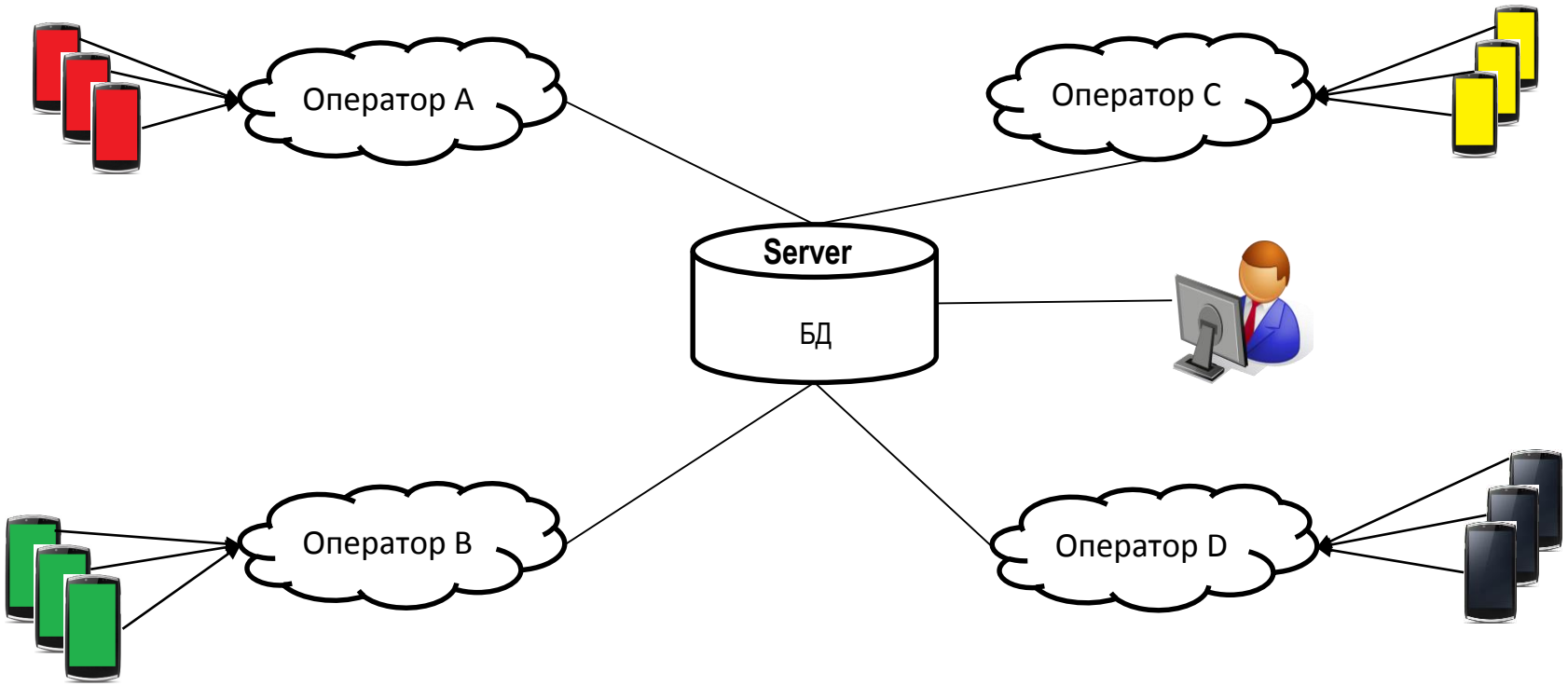
Sandbox даёт результаты:

- Статический анализ и запуск в эмуляторе выявил около 30 ЦУ для мобильного бот-приложения за 2 недели, динамический анализ в песочнице выявил больше 50 ЦУ за сутки.
- Используются более доступные ресурсы для оператора связи - SIM-карты, аппараты, базовая станция, снижая тем самым стоимость создания комплекса и увеличивая аналитическую работу.

* - «Противодействие вредоносному ПО для мобильных устройств на сети оператора связи. Android-honeypot в антифроде»: http://2014.zeronights.ru/assets/files/slides/android_new.zip

Пути решения

Создание координационного центра по обмену данными, выявленных о фродовых схемах, для совершенствования средств для борьбы с мошенничеством.
Основа – доверенный «экспертный центр безопасности*», способный коррелировать данные от крупных телекоммуникационных компаний, банков, платежных систем.



* - Пример концепции создания данного центра (FRAUD-CERT) описан в документах ASMONIA:
http://asmonia.de/deliverables/D4.3_Methods_for_Collaborative_Detection_and_Analysis.pdf

Спасибо за внимание!

Thank you for your attention!

Гончаров Николай
goncharovkolya@list.ru

Горчаков Денис
gorchakov.denis@gmail.com