Николай Гончаров, МТС
Денис Горчаков, Альфа-Банк

# Мобильные бот-сети и противодействие платёжному мошенничеству

# История вопроса

**PHDays III:**
Мошенничество в SMS-банкинге

**ZeroNights 2014:**
Противодействие ВПО для мобильных устройств на сети оператора.
Android Honeypot в антифроде

**AntiFraud Russia-2014:**
Актуальные угрозы фрода в отношении абонентов сотовых сетей связи.
Выявление мобильных бот-сетей

**РусКрипто 2015:**
Расследование инцидентов, связанных с мобильными бот-сетями и вредоносным ПО

**PHDays V:**
Противодействие платёжному фроду на сети оператора связи

# Обстановка

- Android занимает около **80%** рынка.
- Крупнейшие антивирусные лаборатории относят Россию к числу **лидеров** по распространённости и направленности Android-вирусов.
- Схожая статистика по **банковским** вирусам, в том числе мобильным.
- Android Security Report 2015: уровень распространения вредоносного ПО в России **в 3-4 раза выше среднего.**
- На остальных мобильных платформах вредоносные приложения практически отсутствуют, но злоумышленники также обращают на них внимание.

# Способы монетизации

- **Со счёта абонента:** контент-услуги и сервисы мобильных платежей.
- **С привязанных к номеру сервисов:** услуги ДБО (SMS, USSD), платёжные системы.
- **Блокировщики:** crypto / PIN.
- **Нецелевое использование устройств:** спам-рассылки, DDoS, прокси для мошеннической деятельности, SEO.

# Бот-сети

- Большинство современных мобильных вирусов – **полноценные клиенты бот-сетей**: статистика, наборы команд, удалённое управление (head & headless).
- Для противодействия мошенническим схемам можно использовать адаптацию отработанных технологий противодействия компьютерным бот-сетям к мобильным угрозам.

# Угрозы

- Похищение персональных и конфиденциальных данных.
- Фишинг.
- Рассылка спама.
- Анонимный доступ в Сеть.
- Кибершантаж и осуществление DDoS-атаки.
- Получение сведений о местоположении конкретного человека.
- Похищение денег, в том числе используя мобильную коммерцию и контент-услуги

~ 70 тыс. новых жертв ежемесячно в одном регионе.

# Антиотладочные приёмы

- Контроль **IMEI, IMSI** для исключения вызывающей подозрение тарификации и фильтрации/блокировки устройств.
- **Геолокация** (GPS, Wi-Fi, сотовая сеть). Исключение по **SSID, Cell ID,** району.
- Вариация **задержек и сумм** для обхода правил мониторинга. Суточная задержка после заражения.
- **Обфускация:** ProGuard.

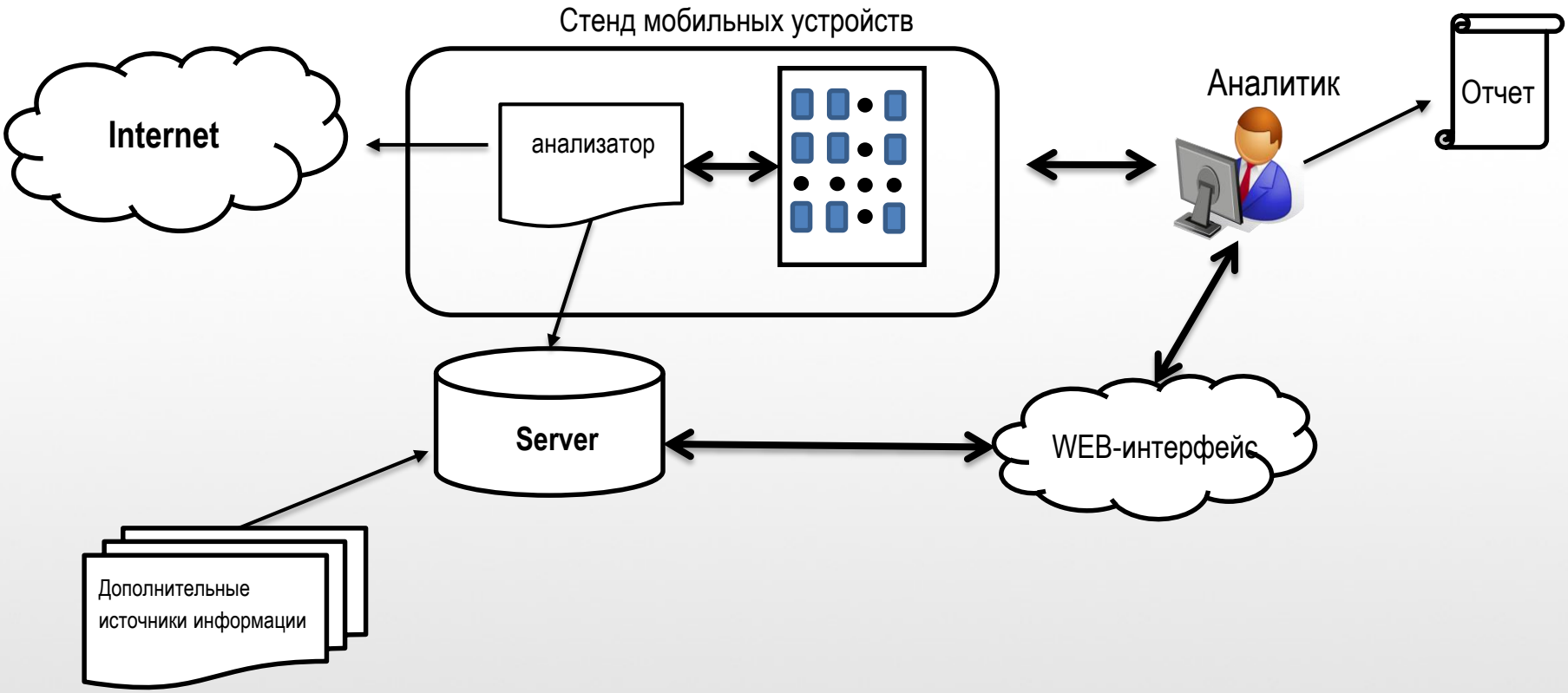
# Антиотладочные приёмы

- Проверка наличия **подключённых сервисов и услуг** не только по истории SMS, но и через отправку тестовых сообщений на короткие номера оператора, банков, платёжных систем.
- **Блокировка абонентских вызовов** на справочные номера: нельзя оперативно пожаловаться в службу поддержки, заблокировать свой счёт, карту.

# Обнаружение

- **Домены и IP:** C&C центры управления, адреса распространения ВПО.
- Сведения о **формате и составе передаваемых данных** на C&C.
- **MSISDN (тел. номера)** – центры управления, коллекторы данных, аккумуляторы денежных средств.
- **Идентификаторы подписок и получателей** для контент-услуг и платёжных сервисов.

# Архитектура



# Botnet monitoring

Анализировать последние: 1 час
Всего запросов за сегодня: 30

**Топ запрашиваемых сайтов**

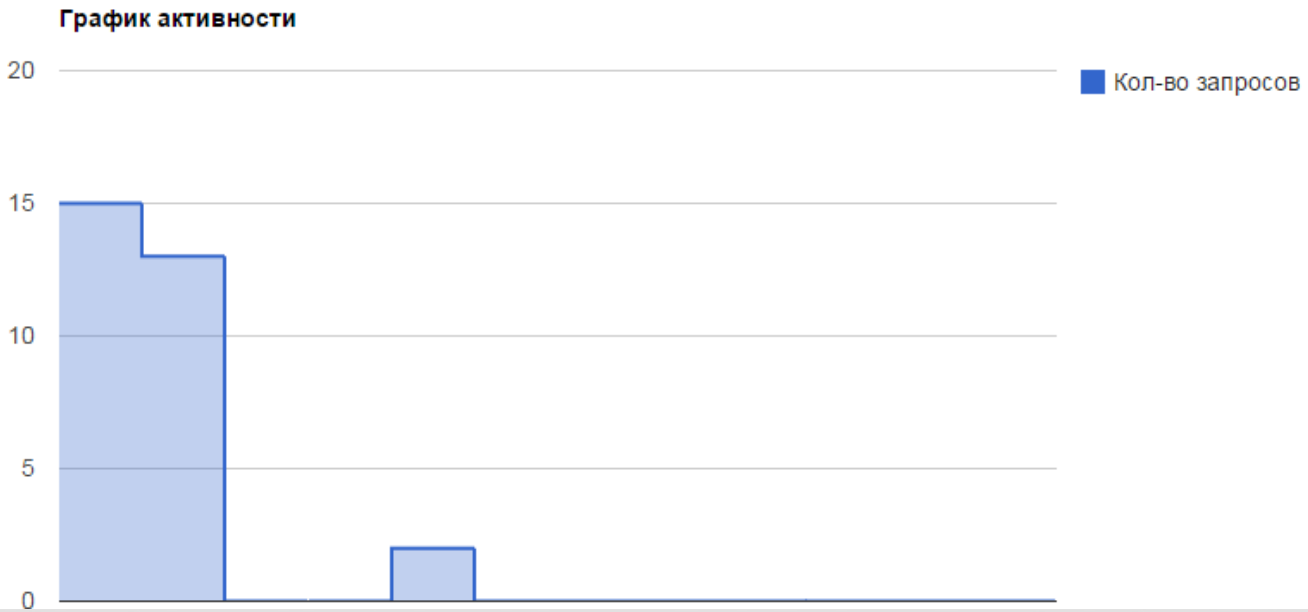
| | |
|---|---|
| www.primebestgoodbeswt.com | 28 |
| lurekaqix.biz | 1 |
| ozozoqimykoric.biz | 1 |

**Топ сайтов с одного приложения**

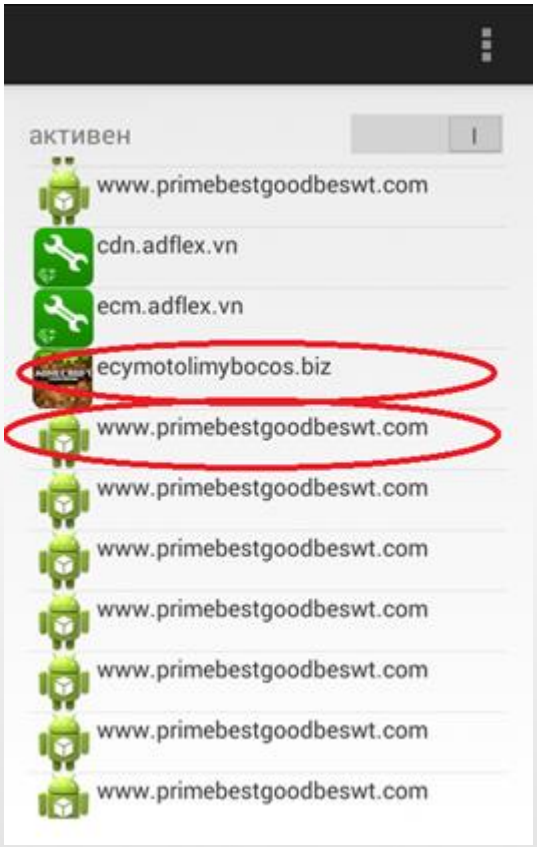
| | | |
|---|---|---|
| MMS-фото | www.primebestgoodbeswt.com | 28 |
| Dragons Rise of Berk | lurekaqix.biz | 1 |
| Dragons Rise of Berk | ozozoqimykoric.biz | 1 |

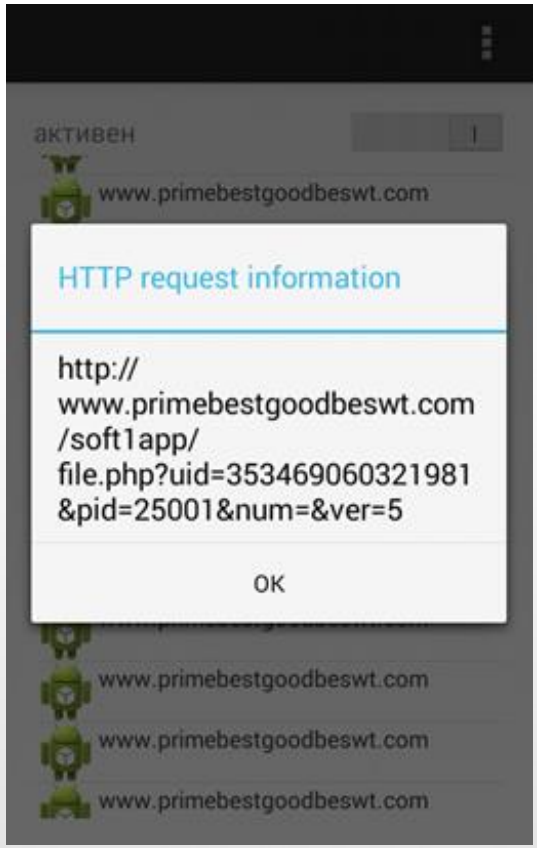
**Топ активных приложений**

| | |
|---|---|
| MMS-фото | 28 |
| Dragons Rise of Berk | 2 |



# Botnet monitoring

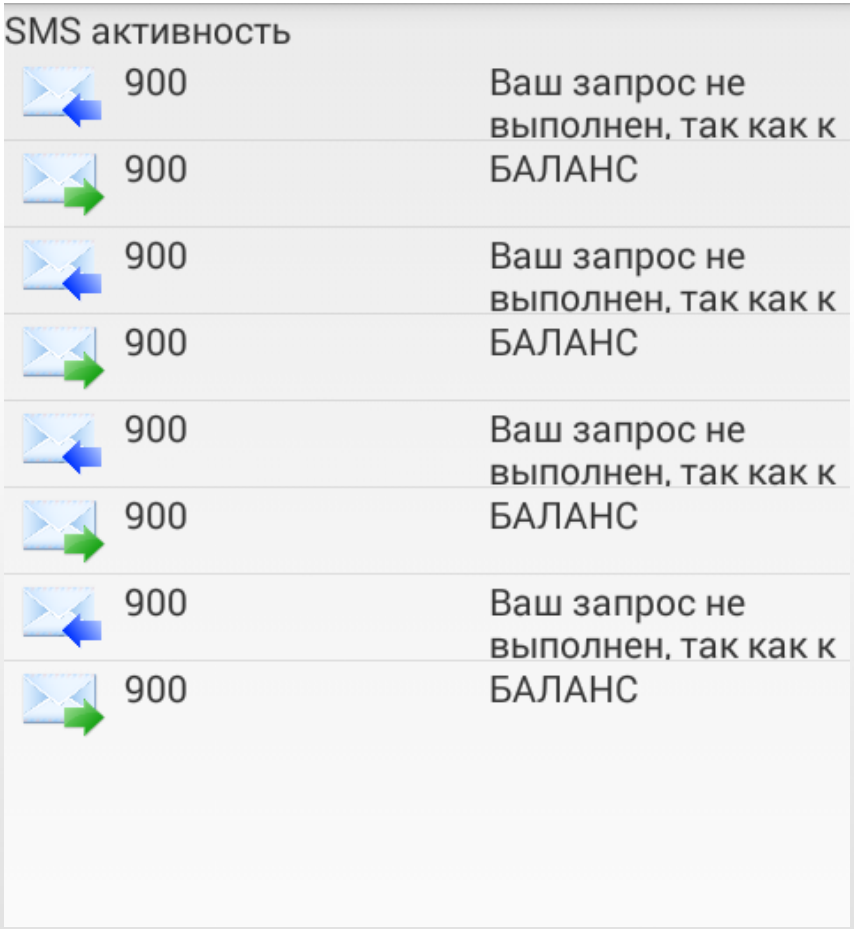


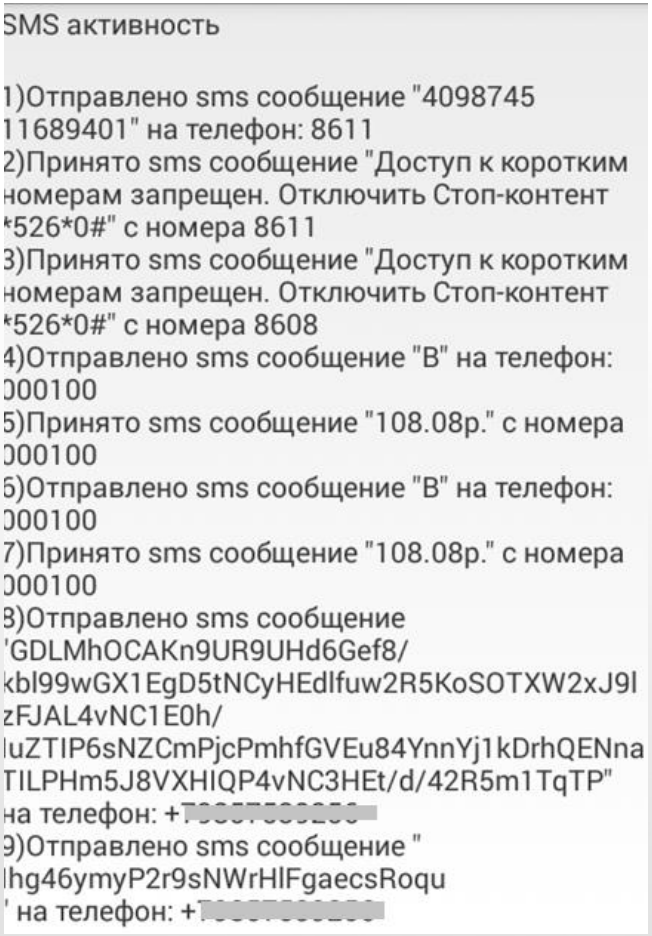



# Botnet monitoring

| Время | URL | Приложение |
|---|---|---|
| 2015-05-19 15:14:59 | www.primebestgoodbeswt.com | MMS-фото |
| URL: | www.primebestgoodbeswt.com/soft1app/sum1.php | |
| Answer: | no answer | |
| 2015-05-19 15:14:58 | www.primebestgoodbeswt.com | MMS-фото |
| URL: | www.primebestgoodbeswt.com/soft1app/file.php?uid=353746021614319&pid=25001&num=&ver=5 | |
| Answer: | {"number":"XXXX","text":"XXXX","stopsms":"1"} | |
| 2015-05-19 15:13:58 | www.primebestgoodbeswt.com | MMS-фото |
| URL: | www.primebestgoodbeswt.com/soft1app/file.php?uid=353746021614319&pid=25001&num=&ver=5 | |
| Answer: | {"number":"XXXX","text":"XXXX","stopsms":"1"} | |

# Подключённые услуги

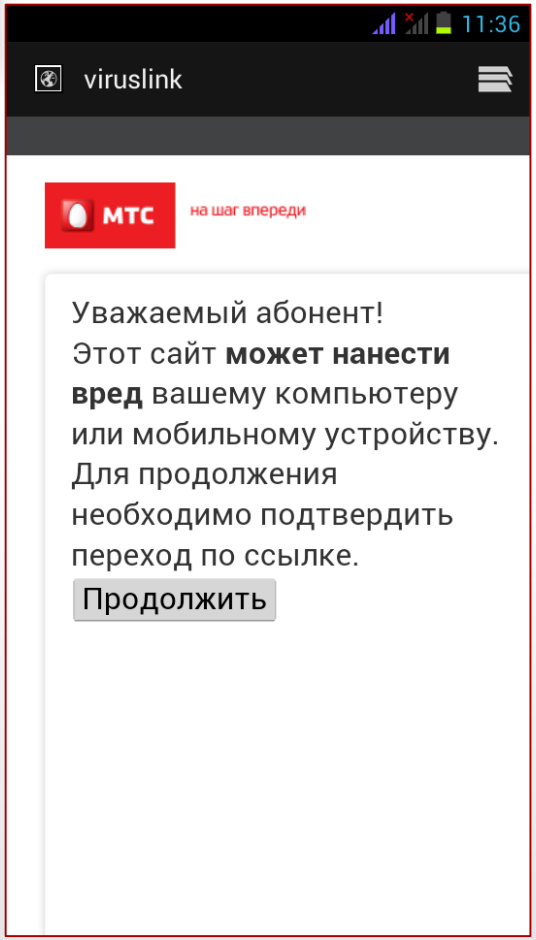


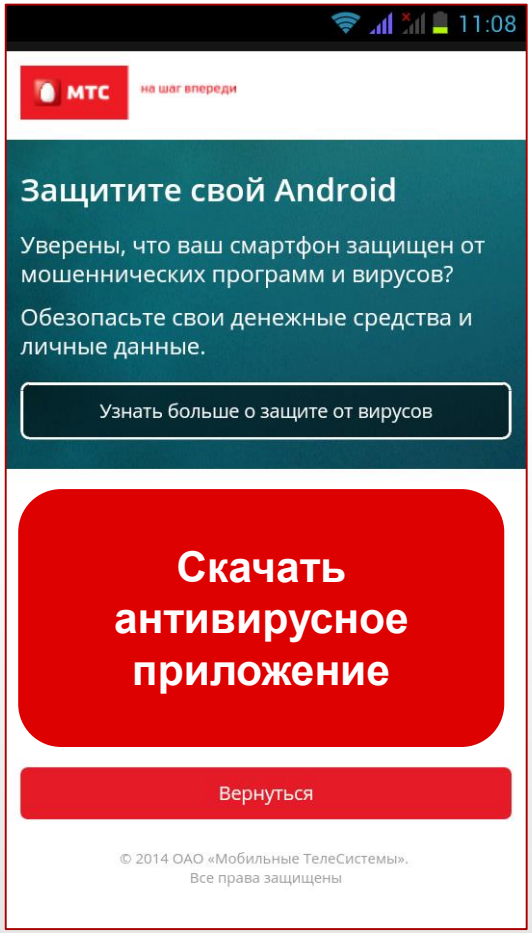



# Преимущества подхода

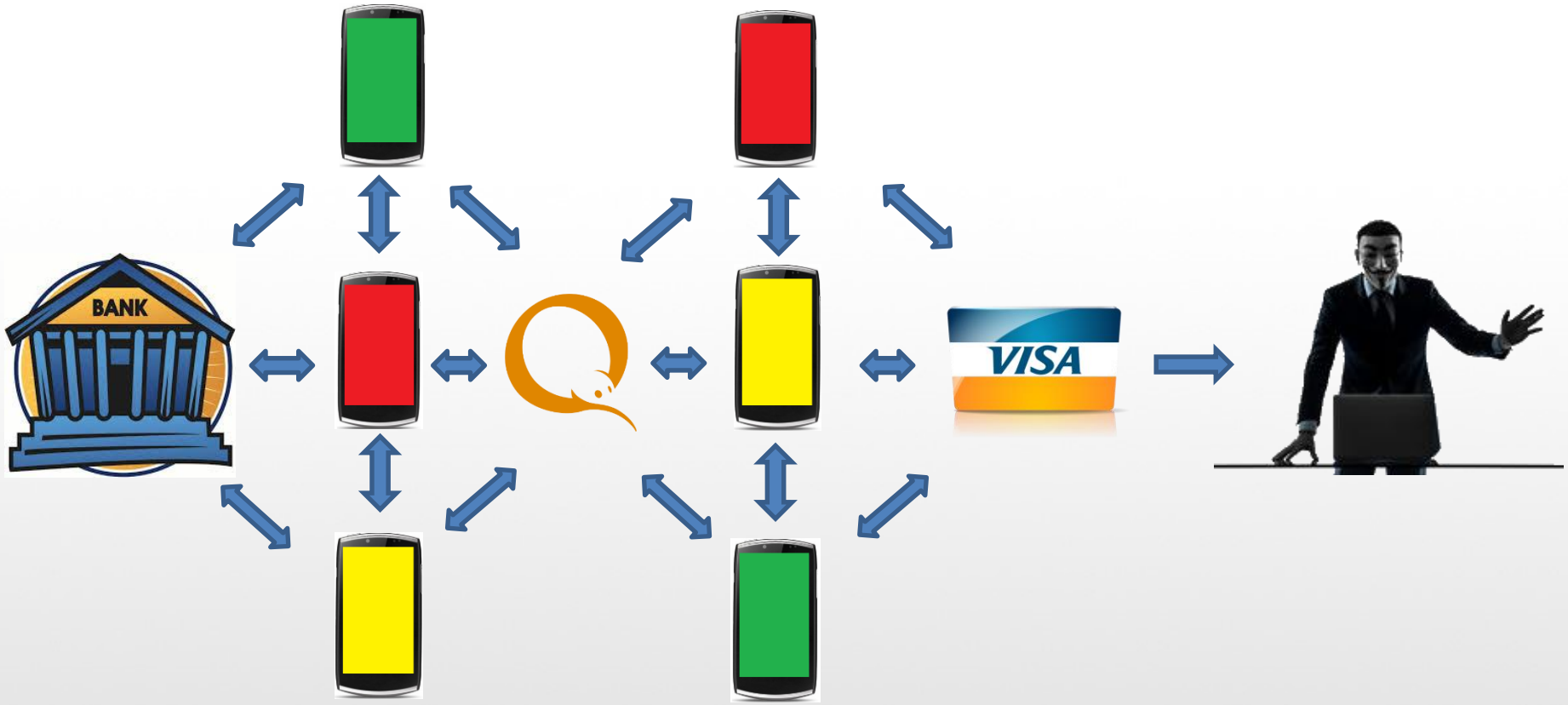
- Основная **цель – оперативное получения информации для быстрого реагирования**. Нас не интересует реверс-инжиниринг вредоносного ПО.
- Экспертный **анализ кода** и **разбор поведения в других программных эмуляторах не обеспечивают полноты** собираемых данных.
- Существует немало **утилит и библиотек для отладки** Android-приложений, однако большинство из них носит **любительский характер и забрасывается** авторами. Велика **сложность доработки и стоимость разработки** силами ИБ-подразделения.

# Защитные меры

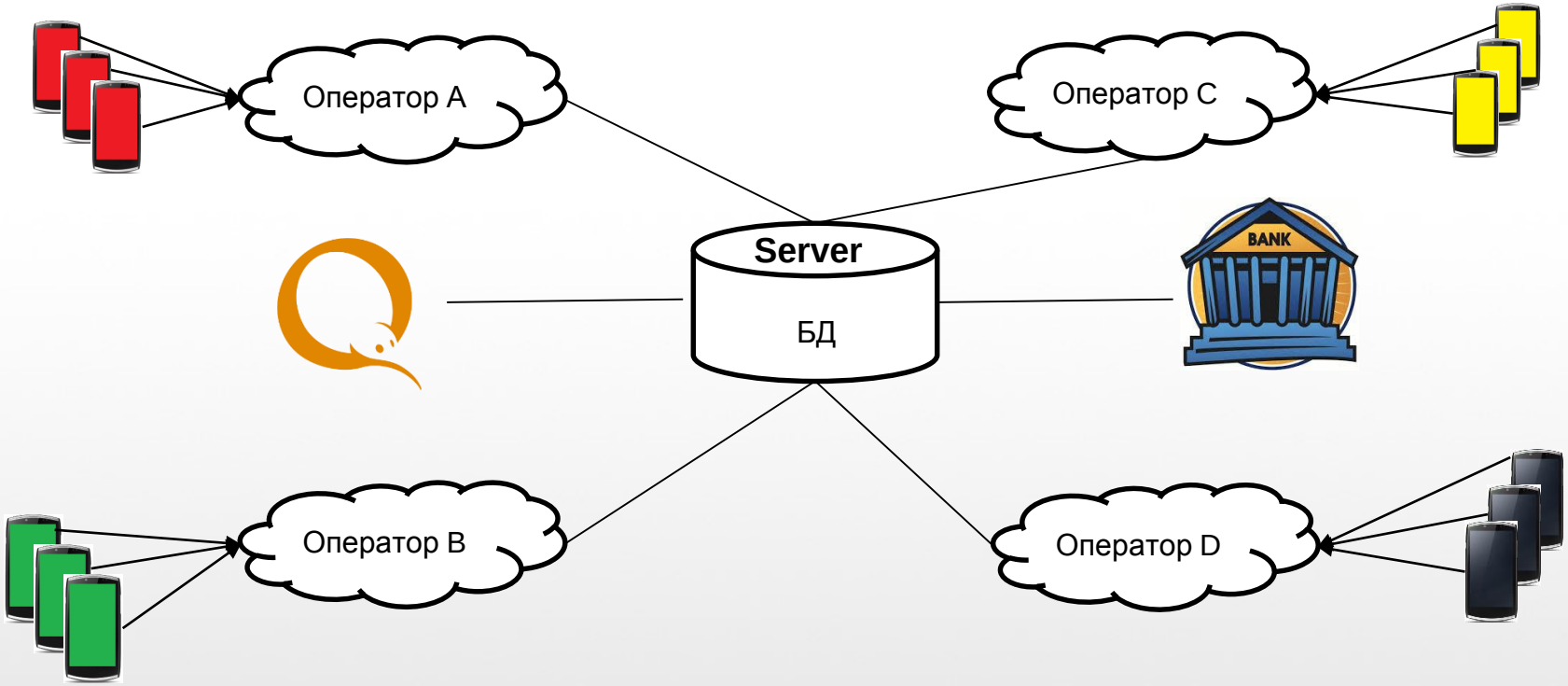


# Типичная схема



# CERT




**ASMONIA:** http://asmonia.de/deliverables/D4.3_Methods_for_Collaborative_Detection_and_Analysis.pdf

*Спасибо за внимание!*

*Thank you for your attention!*

**Гончаров Николай**
nogoncha@mts.ru

**Горчаков Денис**
dgorchakov@alfabank.ru