Николай Гончаров.
Эксперт отдела обеспечения информационной безопасности, ПАО “МТС“.
Аспирант кафедры “Информационная безопасность" МГТУ им. Н.Э. Баумана.

Вредоносное мобильное ПО и бот-сети:

вчера, сегодня, завтра

МТС Ты знаешь, что можешь!

История вопроса

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

InfoSecurity Russia 2015: Техника противодействия платежному мошенничеству на сети оператора связи.

- **Межотраслевой научно-технический журнал «Оборонный комплекс – научно-техническому прогрессу России». 2015/1**

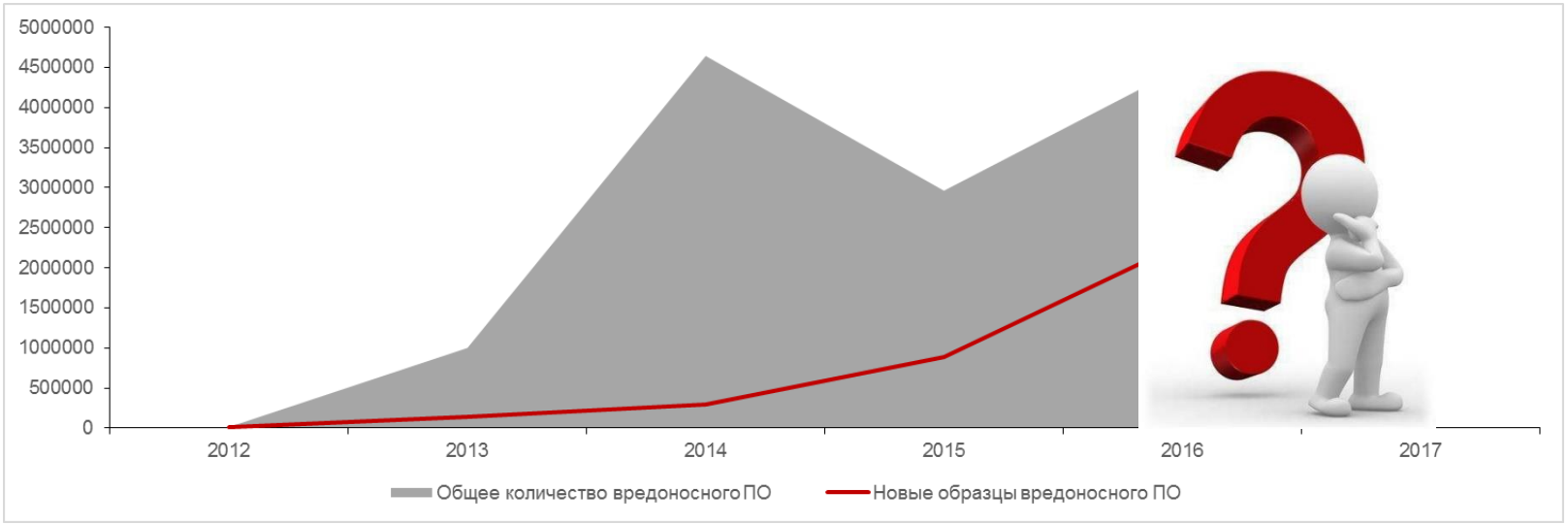
Алгоритм защиты ресурсов телекоммуникационных сетей связи от угроз бот-сетей.

- **Электронный журнал «Молодёжный научно-технический вестник» 2014/10.**

Современные угрозы бот-сетей

Обстановка

- Android занимает лидирующие позиции на рынке, в том числе и по количеству вредоносного ПО.



- На остальных мобильных платформах вредоносные приложения практически отсутствуют, но злоумышленники также обращают на них внимание.
- Россия – лидер по распространённости и направленности мобильных вирусов, в частности банковских троянов.

Угрозы

- Похищение персональных и конфиденциальных данных;
- Фишинг;
- Рассылка спама;
- Анонимный доступ в Сеть;
- Кибершантаж и осуществление DDoS-атак;
- Получение сведений о местоположении конкретного человека;
- Похищение денежных средств, в том числе через сервисы мобильной коммерции и контент-услуги.

Этапы становления

маскировка под топовые приложения, игры, антивирусы

развитие функционала

модифицированные прошивки на серых устройствах

рост вирусов под OS Android

появление массовых мобильных бот-сетей

полноценные клиенты бот-сетей

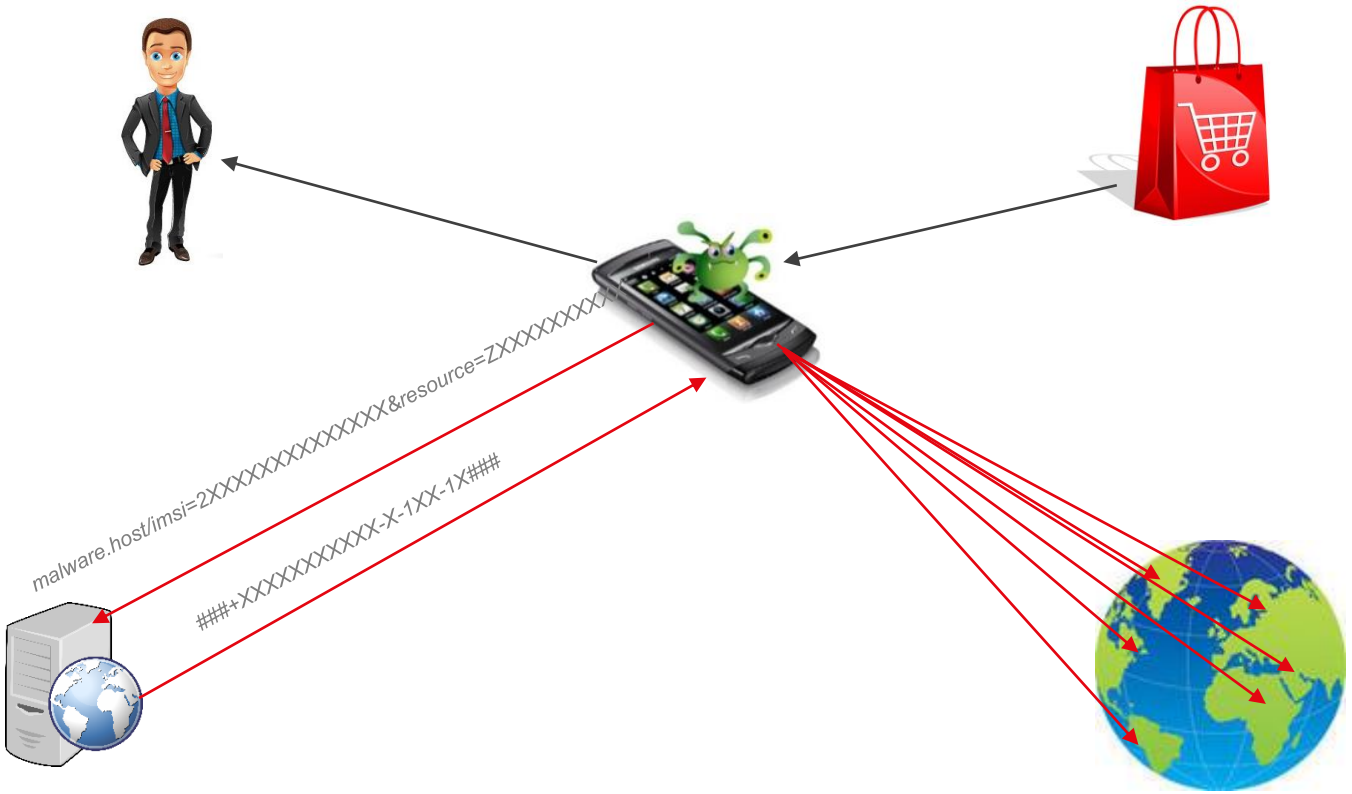
??????

2012г. 2013г. 2014г. 2015г. 2016г.

- sms-трояны
- монетизация через сервисы мобильной коммерции
- монетизация через контент-услуги
- банковские трояны
- фишинг
- воровство данных
- смена вектора - монетизация за счёт показа рекламы
- комбинированные типы методов воздействия и защиты

Функционал вредоносного ПО

Модифицированные прошивки



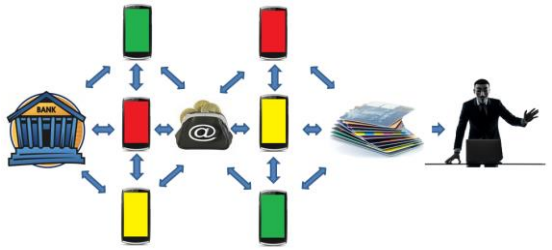
Обнаружение

- 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.
- Анализ кода.
- Проверка в песочницах и эмуляторах.

Современные бот-сети

- Мобильны, многозадачны, легко могут быть перенацелены с одной активности на другую. Одни и те же устройства могут принимать участие в рассылке спама, DDoS-атаках и т.д.

- Центр управления бот-сетью находится в одной сети, жертвы во второй, «коллектор» данных – в третьей. Необходима быстрая и своевременная координация действий в пределах нескольких часов.

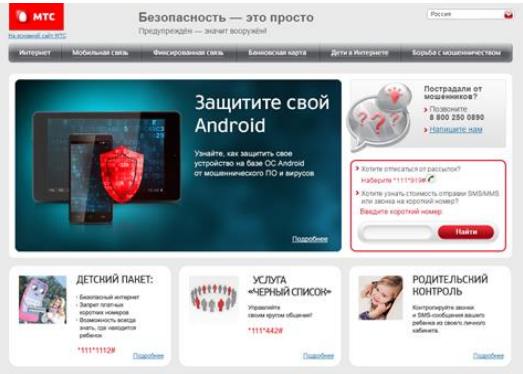


- Корреляция данных: скомпрометированная «учетная запись ДБО» + «зараженный смартфон» + «заражённый компьютер»

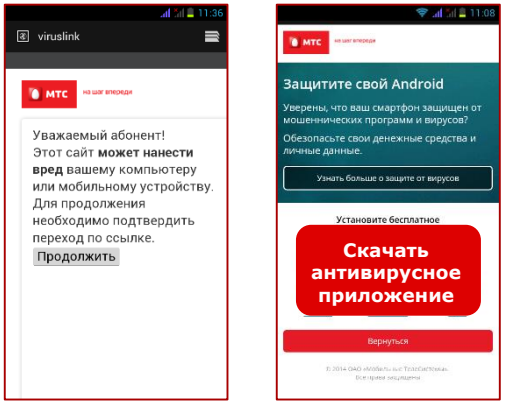
- Проблема затрагивает всех участников рынка – в одну мошенническую цепочку попадают банки, платежные системы, операторы, что затрудняет расследование инцидентов.

Действия МТС по противодействию угрозам

Инфо-портал safety.mts.ru



Предупреждение абонентов

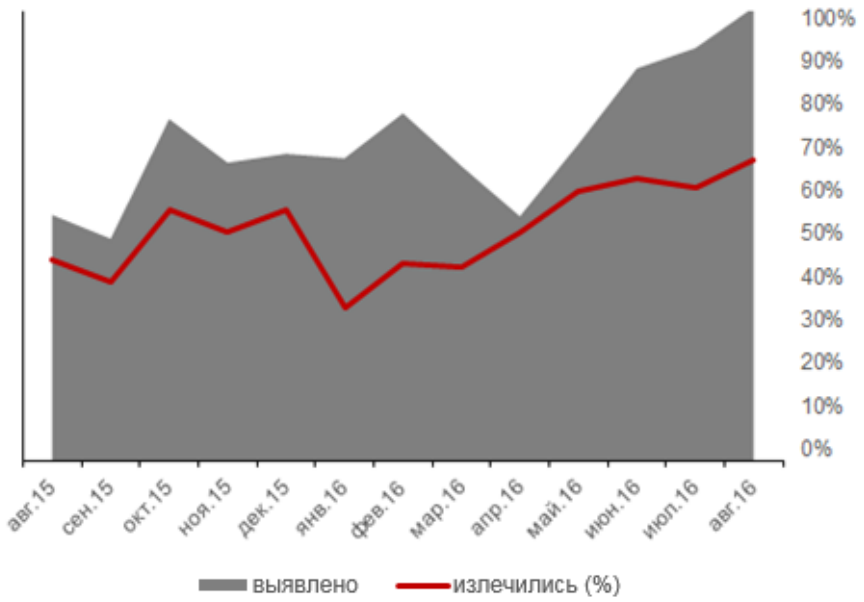


- Инфо-портал safety.mts.ru с информацией об актуальных угрозах и мерах по защите.
- Мониторинг вирусной активности на сети МТС, выявление вредоносных приложений и центров управления бот-сетями.
- Предупреждение абонентов МТС при попытке перехода по ссылке на мошенническое или вредоносное ПО.
- Блокировка СМС рассылок с вредоносными ссылками.
- Выявление зараженных абонентов МТС и информирование об угрозах.

Безопасность абонентов МТС обеспечивается своевременным информированием, блокированием вредоносных рассылок и повышением осведомленности абонентов об актуальных угрозах и способах защиты.

Результаты защиты абонентов МТС

Результаты мер по защите мобильных устройств от вредоносного ПО., тыс.



Блокировка вредоносных ссылок (I-II кв 2016):

- Выявлено и **заблокировано более 3,5 тысяч ссылок на вредоносные программы** и адресов серверов злоумышленников.
- **Предотвращено более 1,8 миллиарда абонентских переходов** на данные ссылки и сервера.

Информирование абонентов (I-II кв 2016):

- **Объем аудитории** составил **более одного миллиона абонентов**.
- По результатам кампаний **более 60%** проинформированных абонентов **принимают меры по защите** своих мобильных устройств от вредоносного ПО.

Для защиты абонентов МТС реализует комплекс мер по выявлению угроз, а также повышению осведомленности абонентов.

Спасибо за внимание!

Николай Гончаров
nogoncha@mts.ru

МТС Ты знаешь, что можешь!