Dr.WEB®
с 1992 года

# Обзор вирусной активности для мобильных Android-устройств за март 2015 года

# Обзор вирусной активности для мобильных Android-устройств за март 2015 года

2 апреля 2015 года

## Главные тенденции марта

- Активность СМС-троянцев
- Распространение троянцев-банкеров
- Рост числа троянцев-вымогателей
- Появление новых вредоносных программ, созданных киберпреступниками для получения незаконного заработка

### Количество записей для вредоносных и нежелательных программ под ОС Android в вирусной базе Dr.Web

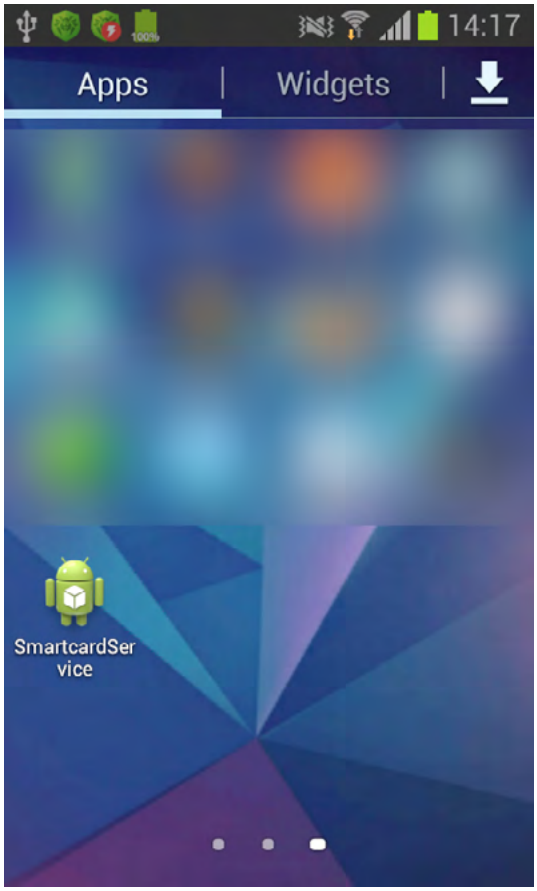
| Февраль 2015 | Март 2015 | Динамика |
|---|---|---|
| 6665 | 7103 | +6,57% |

# Обзор вирусной активности для мобильных Android-устройств за март 2015 года

## «Мобильная» угроза месяца

В прошедшем месяце специалисты компании «Доктор Веб» обнаружили опасного многофункционального троянца **Android.Titan.1**, предназначенного для незаметной отправки СМС-сообщений, совершения телефонных звонков, а также сбора различной конфиденциальной информации. Особенности данного троянца:

- Может распространяться злоумышленниками через облачные сервисы с использованием нежелательных СМС, содержащих ссылку на загрузку вредоносного приложения.
- После запуска на мобильных устройствах удаляет свой ярлык, скрываясь от пользователей.
- Способен незаметно выполнять телефонные звонки, в том числе когда зараженный смартфон или планшет находится в режиме ожидания с выключенным экраном. При этом во время совершаемого троянцем телефонного разговора экран остается неактивным, в результате чего пользователь не подозревает о нежелательной деятельности зараженного устройства.
- Основной вредоносный функционал реализован в виде отдельной Unix-библиотеки, поэтому некоторые антивирусные приложения могут оказаться не в состоянии обнаружить троянца.

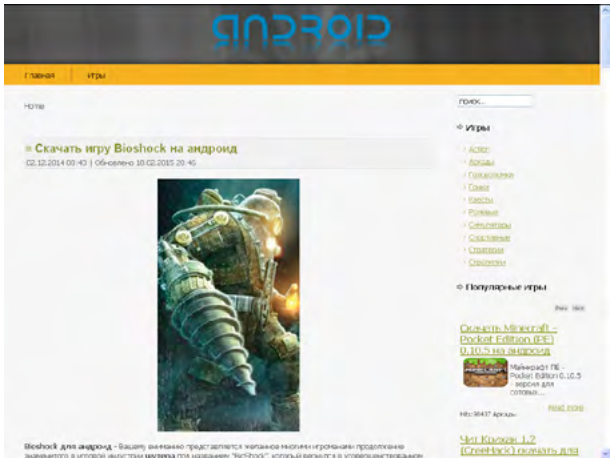



Данная вредоносная программа успешно обнаруживается и нейтрализуется антивирусными продуктами Dr.Web для Android. Подробнее о троянце рассказано в соответствующей публикации на сайте компании.

# Обзор вирусной активности для мобильных Android-устройств за март 2015 года

## СМС-троянцы

Одними из наиболее активных вредоносных Android-программ по-прежнему остаются различные СМС-троянцы. В марте самыми заметными из них стали представители семейства **Android.Bodkel**, часть которых распространялась вирусописателями при помощи популярной в России социальной сети. Злоумышленники создали в ней несколько мошеннических сообществ, посвященных пиратским или якобы бесплатным версиям платного ПО для ОС Android, и предлагали потенциальным жертвам посетить ряд сомнительных веб-сайтов для загрузки подобных программ.


После установки на устройства пользователей эти вредоносные приложения по команде злоумышленников могли незаметно отправлять дорогостоящие СМС-сообщения, автоматически подписывать абонентов на платные услуги, обходя защитный сервис captcha, а также выполнять широкий спектр других опасных действий. Некоторые троянцы семейства **Android.Bodkel**, использованные в данной атаке:

- Android.Bodkel.123
- Android.Bodkel.162
- Android.Bodkel.166
- Android.Bodkel.167

Число записей для СМС-троянцев Android. Bodkel в вирусной базе Dr.Web:

| Февраль 2015 | Март 2015 | Динамика |
|---|---|---|
| 154 | 169 | +9,74% |

# Обзор вирусной активности для мобильных Android-устройств за март 2015 года

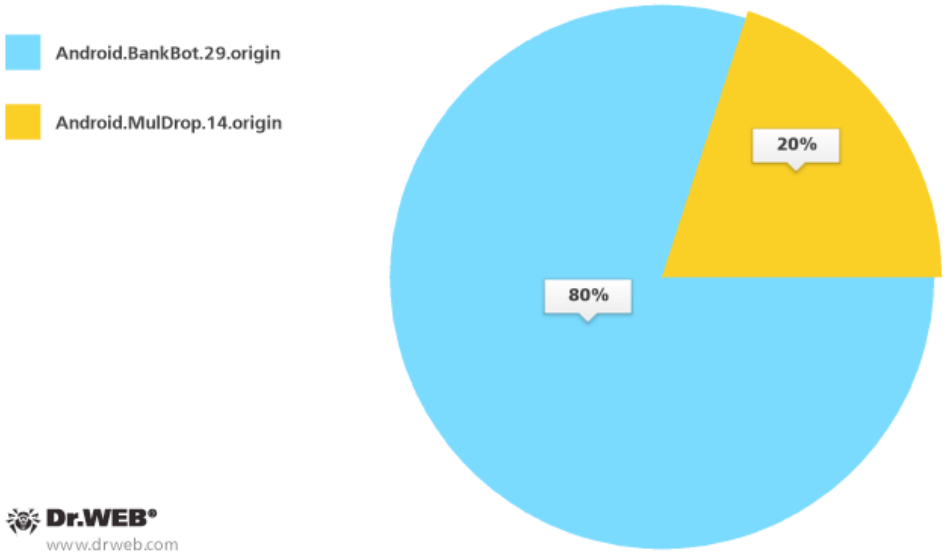
Также в прошедшем месяце вирусописатели продолжили активно создавать и распространять среди пользователей СМС-троянцев семейства Android.SmsSend. Число записей для этих вредоносных программ в вирусной базе Dr.Web:

| Февраль 2015 | Март 2015 | Динамика |
|---|---|---|
| 3264 | 3529 | +8,12% |

## Банковские троянцы

В прошедшем месяце были зафиксированы новые случаи распространения злоумышленниками разнообразных банковских троянцев для ОС Android. В частности, подобные вредоносные приложения были в очередной раз задействованы при атаках на пользователей из Южной Кореи – здесь киберпреступники вновь применяли рассылку СМС-сообщений, содержащих ссылку на загрузку вредоносных программ, однако число подобных спам-кампаний в марте заметно сократилось по сравнению с предыдущими месяцами и составило менее 20 случаев. Вирусописатели использовали следующие вредоносные Android-приложения при атаках на южнокорейских клиентов банков:

Android-троянцы, распространяемые среди южнокорейских пользователей при помощи СМС-спама



# Обзор вирусной активности для мобильных Android-устройств за март 2015 года

### Android.BankBot.29.origin

Банковский троянец, крадущий аутентификационные данные у клиентов ряда южнокорейских кредитных организаций. При запуске оригинальных программ интернет-банкинга троянец подменяет их интерфейс своей поддельной копией, в которой запрашиваются все конфиденциальные сведения, необходимые для доступа к управлению банковским счетом. Введенная пользователем информация в дальнейшем передается злоумышленникам. Под видом подписки на некую банковскую услугу пытается установить вредоносную программу Android.Banker.32.origin.

### Android.MulDrop.14.origin

Троянская программа, предназначенная для распространения и установки на мобильные Android-устройства других вредоносных программ, в частности, различных банковских троянцев. Распространяется преимущественно среди южнокорейских пользователей.

## Трояны-вымогатели

В марте были обнаружены новые трояны-вымогатели семейства Android.Locker, блокирующие мобильные устройства под управлением ОС Android и требующие у пользователей выкуп за их разблокировку. Число записей для этих опасных вредоносных программ в вирусной базе Dr.Web:

| Февраль 2015 | Март 2015 | Динамика |
|---|---|---|
| 174 | 190 | +9,2% |

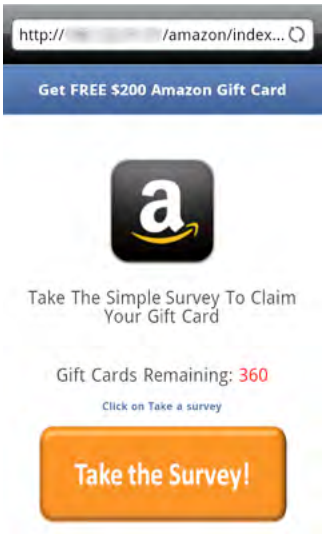
# Обзор вирусной активности для мобильных Android-устройств за март 2015 года

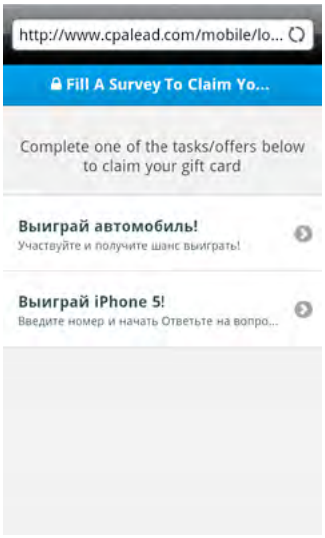
## Другие вредоносные приложения

### Android.Gazon.1

Троянская программа, предназначенная для незаконного заработка злоумышленников посредством загрузки в веб-браузере мобильного Android-устройства различных опросов. Особенности троянца:

- Распространяется вирусописателями под видом купона на скидку для онлайн-магазина Amazon. При этом троянец способен распространяться среди пользователей самостоятельно благодаря наличию функционала СМС-червя. Для этого вредоносная программа отправляет всем контактам из телефонной книги жертвы СМС-сообщения, в которых для получения «купона» предлагается перейти по ссылке.
- После запуска загружает в веб-браузере мобильного устройства страницу с тем или иным опросом, после прохождения которого пользователем авторы вредоносного приложения получают денежное вознаграждение.


### Android.Backdoor.160.origin

Многофункциональный троянец-бэкдор для ОС Android, способный выполнять широкий спектр задач. Особенности:

- Управляется злоумышленниками при помощи push-уведомлений сервиса Baidu Cloud.
- Способен перехватывать СМС, производить аудиозапись при помощи встроенного в мобильное устройство микрофона, определять местоположение пользователя, загружать на удаленный сервер фотографии жертвы, а также все ее контакты из телефонной книги.
- Может отправлять СМС, совершать звонки, загружать и удалять файлы.
- Имеет несколько модификаций (**Android.Backdoor.161.origin, Android.Backdoor.165.origin**).

# Обзор вирусной активности для мобильных Android-устройств за март 2015 года

## О компании «Доктор Веб»

«Доктор Веб» — российский производитель антивирусных средств защиты информации под маркой Dr.Web. Продукты Dr.Web разрабатываются с 1992 года. Компания — ключевой игрок на российском рынке программных средств обеспечения базовой потребности бизнеса — безопасности информации.

«Доктор Веб» — один из немногих антивирусных вендоров в мире, владеющих собственными уникальными технологиями детектирования и лечения вредоносных программ. Компания имеет свою антивирусную лабораторию, глобальную службу вирусного мониторинга и службу технической поддержки.

Стратегической задачей компании, на которую нацелены усилия всех сотрудников, является создание лучших средств антивирусной защиты, отвечающих всем современным требованиям к этому классу программ, а также разработка новых технологических решений, позволяющих пользователям встречать во всеоружии любые виды компьютерных угроз.

**Полезные ресурсы**
ВебIQметр | Центр противодействия кибер-мошенничеству

**Пресс-центр**
Официальная информация | Контакты для прессы | Брошюры | Галерея

**Контакты**
Центральный офис
125124, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп.12а
www.антивирус.рф | www.drweb.ru | www.mobi.drweb.com | www.av-desk.ru
«Доктор Веб» в других странах