Dr.WEB®
с 1992 года

Обзор вирусной активности для мобильных Android-устройств в апреле 2015 года

Обзор вирусной активности для мобильных Android-устройств в апреле 2015 года

30 апреля 2015 года

Главные тенденции апреля

- Распространение опасного троянца Android.Toorch.1.origin, способного получить root-доступ для незаметной загрузки, установки и удаления программ
- Обнаружение в каталоге Google play очередных приложений с агрессивным рекламным модулем
- Высокая активность троянцев-банкеров

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

Март 2015	Апрель 2015	Динамика
7103	7971	+12,22%

Обзор вирусной активности для мобильных Android-устройств в апреле 2015 года

«Мобильная» угроза месяца

В прошедшем месяце специалисты компании «Доктор Веб» исследовали опасного троянца Android.Toorch.1.origin, предназначенного для незаметной загрузки, установки и удаления приложений, а также способного отображать на экране зараженных мобильных устройств навязчивую рекламу. Особенности троянца:

- распространяется злоумышленниками под видом безобидного приложения-фонарика, в действительности выполняющего указанную функцию;
- передает киберпреступникам различную конфиденциальную информацию, включая GPS-координаты зараженного устройства;
- способен получить root-доступ и по команде вирусописателей незаметно выполнять установку и удаление заданных ими приложений;
- помещает в системный каталог дополнительные вредоносные компоненты;
- может отображать навязчивую рекламу.

Обзор вирусной активности для мобильных Android-устройств в апреле 2015 года

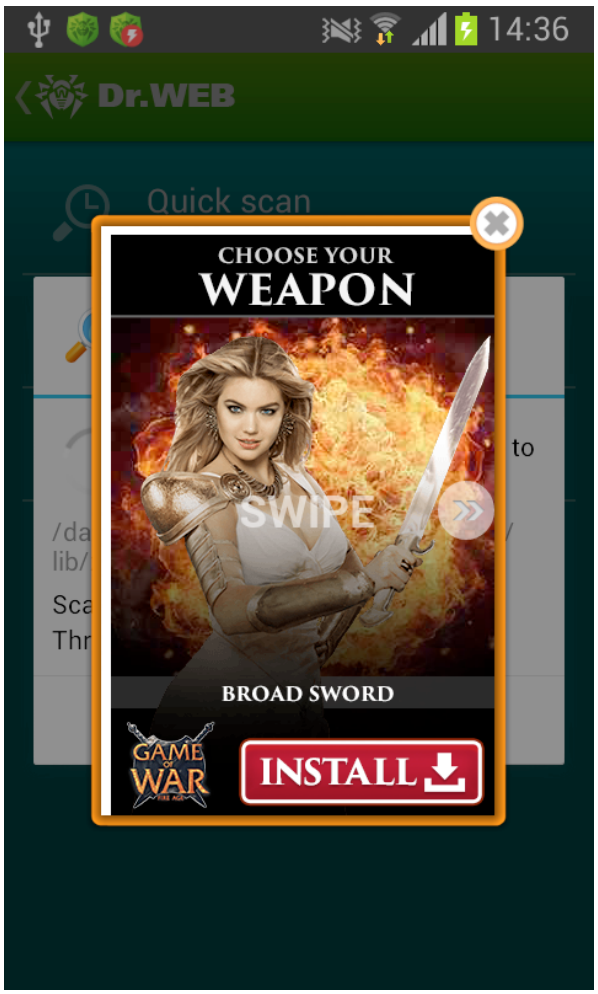
В случае обнаружения Android.Toorch.1.origin на мобильном устройстве пользователям настоятельно рекомендуется выполнить полное сканирование системы Антивирусом Dr.Web для Android с целью выявления всех вспомогательных компонентов троянца. Чтобы окончательно удалить инсталлированные вредоносным приложением модули, необходимо загрузить разработанную специалистами компании «Доктор Веб» утилиту, установить ее, запустить и следовать инструкциям на экране. Подробнее об этом троянце можно прочесть в соответствующей публикации.

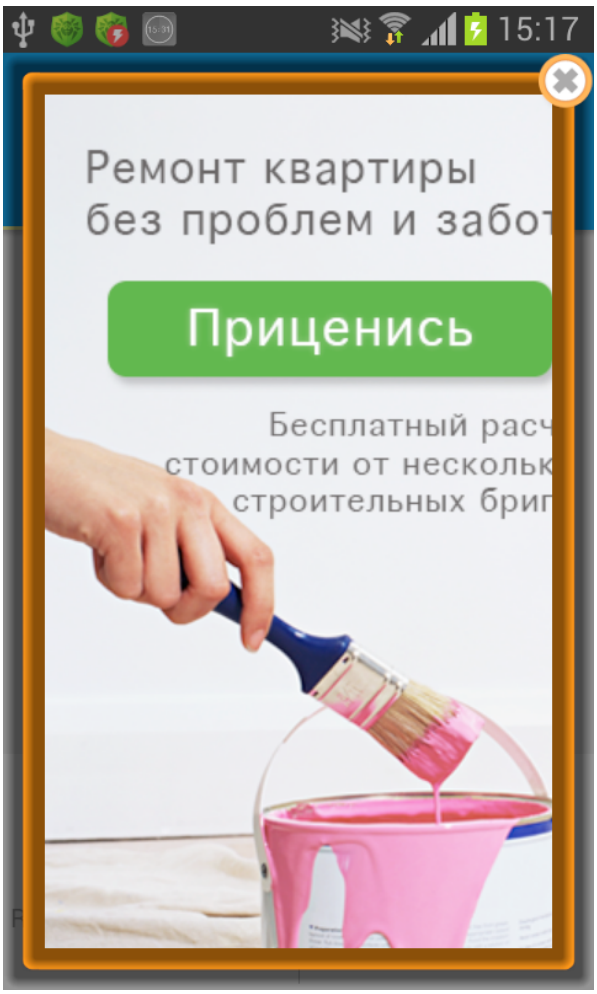
Обзор вирусной активности для мобильных Android-устройств в апреле 2015 года

Агрессивные рекламные модули

В апреле в каталоге Google play вновь были выявлены приложения, содержащие агрессивный рекламный модуль, в частности, Adware.MobiDash.2.origin. Специалисты «Доктор Веб» обнаружили несколько
подобных программ, при этом суммарное число их загрузок превысило
2 500 000. Система Adware.MobiDash.2.origin используется разработчиками бесплатного ПО с целью его монетизации и предназначена для показа разнообразной рекламы. Она способна выполнять следующие
нежелательные действия:

- отображение на экране мобильного устройства различных баннеров, которые размещаются в том числе и поверх окон других работающих программ;
- открытие в веб-браузере ведущих на рекламные ресурсы ссылок;
- демонстрация рекламных и иных сообщений в панели уведомлений.





Обзор вирусной активности для мобильных Android-устройств в апреле 2015 года

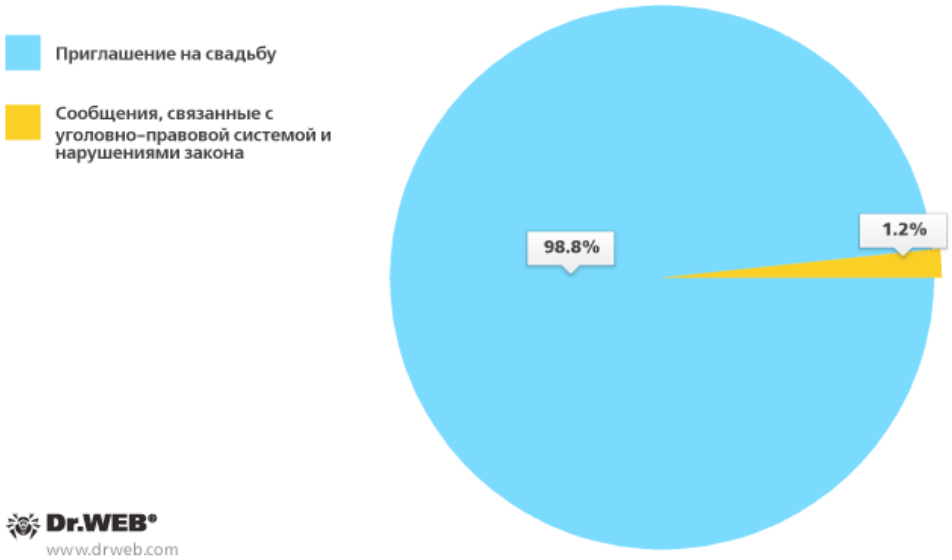
Число записей для «мобильных» рекламных модулей в вирусной базе Dr.Web:

Март 2015	Апрель 2015	Динамика
123	144	+17,1%

Банковские троянцы

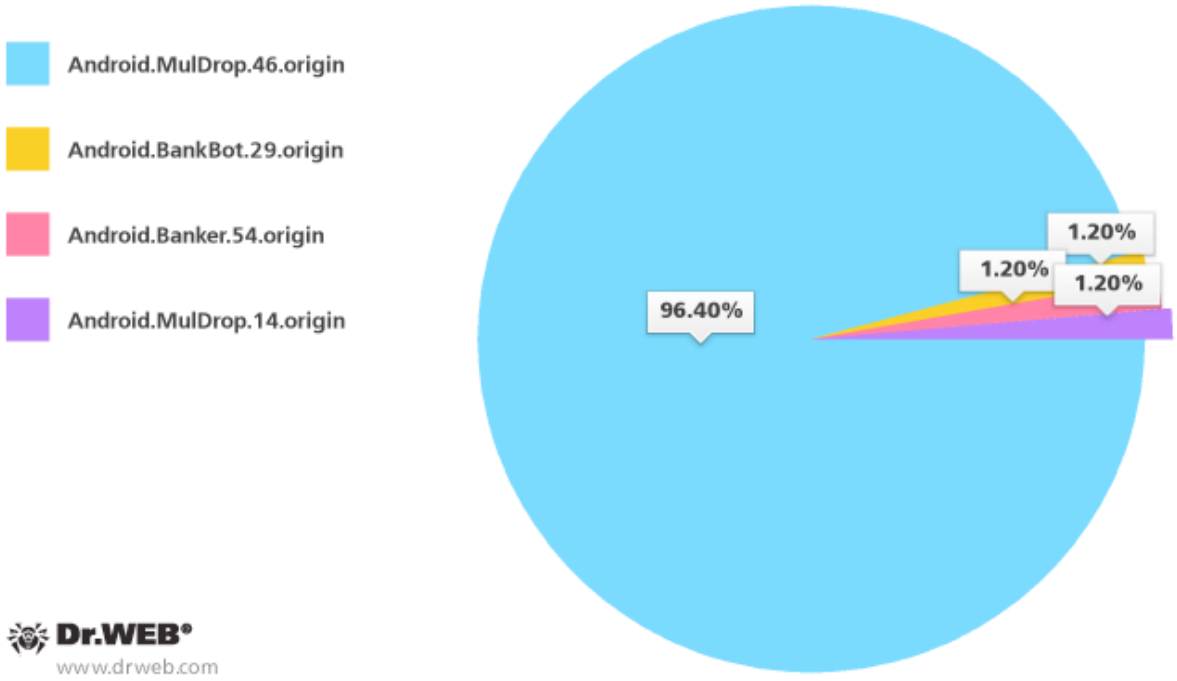
Высокую активность в апреле вновь проявили разнообразные банковские троянцы, заражающие Android-смартфоны и планшеты и атакующие пользователей по всему миру. Так, для распространения банкеров среди жителей Южной Кореи злоумышленники в очередной раз применяли рассылку нежелательных СМС, в которых указывалась ссылка на загрузку того или иного вредоносного приложения. Специалисты компании «Доктор Веб» зафиксировали более 80 подобных спам-кампаний, при этом киберпреступники использовали следующую тематику нежелательных сообщений:

Тематика нежелательных СМС-сообщений, применявшихся при распространении вредоносных программ в Южной Корее



Обзор вирусной активности для мобильных Android-устройств в апреле 2015 года

Вредоносные приложения, задействованные в данных атаках:



Android.MulDrop.46.origin

Троянская программа, предназначенная для доставки на мобильные устройства и последующего запуска других вредоносных приложений, в частности, банкеров. Может распространяться злоумышленниками под видом популярного веб-браузера или иного легитимного ПО.

Android.BankBot.29.origin

Банковский троянец, крадущий аутентификационные данные у клиентов ряда южнокорейских кредитных организаций. При запуске оригинальных программ интернет-банкинга 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 приложений, в частности, различных банковских троянцев. Распространяется преимущественно среди южнокорейских пользователей.

Обзор вирусной активности для мобильных Android-устройств в апреле 2015 года

Также в прошедшем месяце специалисты компании «Доктор Веб» зафиксировали высокую активность банковских троянцев семейства Android.BankBot, предназначенных для атаки на клиентов кредитных организаций по всему миру. В начале апреля деятельность распространявшей данные вредоносные приложения преступной группы была пресечена, но это не помешало другим злоумышленникам продолжить использование данного типа банкеров.

Число записей для банковских троянцев Android.BankBot в вирусной базе Dr.Web:

Март 2015	Апрель 2015	Динамика
94	110	+17,02%

Многие троянцы Android.BankBot опасны не только тем, что способны автоматически выполнять кражу денег с банковских счетов пользователей, но также обладают функционалом, позволяющим им блокировать работу популярных антивирусных приложений. Компания «Доктор Веб» выпустила специальное обновление своих антивирусных продуктов для ОС Android, в котором реализован механизм противодействия подобным атакам, поэтому пользователи Антивируса Dr.Web для Android и Антивируса Dr.Web для Android Light по-прежнему находятся под надежной защитой.

Обзор вирусной активности для мобильных Android-устройств в апреле 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