Dr.WEB®
с 1992 года

Обзор вирусной активности для мобильных Android-устройств за январь 2015 года

Обзор вирусной активности для мобильных Android-устройств за январь 2015 года

2 февраля 2015 года

Главные тенденции января

- Активность банковских троянцев.
- Появление новых программ-шпионов.
- Наличие в каталоге Google Play программ, использующих агрессивные рекламные системы.
- Дальнейшее распространение троянцев, внедренных злоумышленниками в прошивку операционной системы или непосредственно на мобильное устройство.

Новые записи в вирусной базе Dr.Web для ОС Android

	Вредоносное ПО	Программы-шпионы	Рекламные модули
Январь 2015	351	11	13

Обзор вирусной активности для мобильных Android-устройств за январь 2015 года

«Мобильная» угроза месяца

Троянец Android.CaPson.1

- Может распространяться внутри модифицированной злоумышленниками Android-прошивки.
- Представляет собой исполняемый Linux-файл, который при запуске извлекает из себя несколько рабочих модулей, часть из которых зашифрована. После того как эти компоненты будут расшифрованы и загружены в оперативную память, троянская программа удаляет исходные файлы и приступает к вредоносной деятельности.
- Способен незаметно отправлять и перехватывать СМС-сообщения, открывать интернет-страницы, передавать на удаленный сервер информацию о зараженном мобильном устройстве, а также загружать другие приложения.

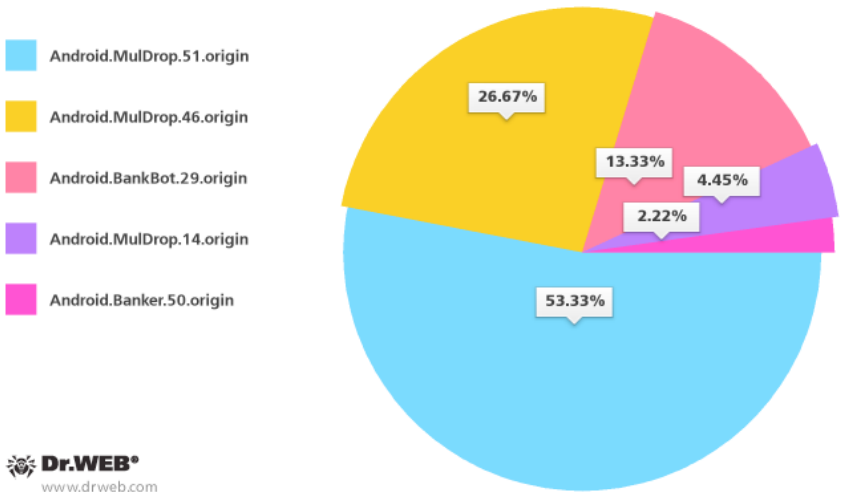
Обзор вирусной активности для мобильных Android-устройств за январь 2015 года

Банковские Android-троянцы

В прошедшем месяце специалисты компании «Доктор Веб» отметили появление очередных банковских троянцев, атакующих пользователей мобильных Android-устройств. Немалую активность подобные вредоносные приложения вновь проявили в Южной Корее, где для распространения Android-троянцев злоумышленники активно используют содержащие ссылку на их загрузку СМС-сообщения.

Выявлено более 40 подобных спам-кампаний, в которых было задействовано несколько вредоносных программ.

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



Обзор вирусной активности для мобильных Android-устройств за январь 2015 года

- **Троянцы Android.MulDrop**
  Вредоносные программы, предназначенные для распространения и установки на мобильные устройства других Android-троянцев. Южнокорейскими вирусописателями данные вредоносные приложения используются для распространения разнообразных троянцев-банкеров.
- **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.Banker.50.origin**
  Представитель семейства банковских троянцев, предназначенных для кражи денежных средств со счетов пользователей ОС Android.

Обзор вирусной активности для мобильных Android-устройств за январь 2015 года

ПО для кибершпионажа

Проблема кибершпионажа остается весьма актуальной для пользователей мобильных устройств. В январе вирусная база Dr.Web пополнилась большим числом записей для разнообразных коммерческих шпионских приложений, предназначенных для установки на Android-смартфоны и планшеты и осуществления слежки за их владельцами. Наряду с обнаружением новых представителей известных семейств «мобильных» программ-шпионов, таких как P**rogram.MobileSpy, Program.Tracer, Program.Highster, Program.OwnSpy, Program.MSpy** и ряда других, специалисты компании «Доктор Веб» проанализировали и новые программы подобного класса, например, **Program.ZealSpy.1.origin, Program.LetMeSpy.1.origin и Program.CellSpy.1.origin.**

Program.ZealSpy.1.origin

- Перехватывает СМС- и email-сообщения
- Получает информацию о телефонных звонках и контактах пользователей
- Отслеживает GPS-координаты
- Считывает переписку в популярных программах обмена сообщениями и т. п.

Program.LetMeSpy.1.origin

Эта вредоносная программа способна отслеживать:

- СМС-сообщения;
- телефонные звонки;
- GPS-координаты Android-устройств.

Program.CellSpy.1.origin

- Перехватывает СМС-сообщения и телефонные звонки
- Получает GPS-координаты устройства
- Ведет скрытую аудиозапись окружения
- Просматривает историю посещений веб-браузера

Обзор вирусной активности для мобильных Android-устройств за январь 2015 года

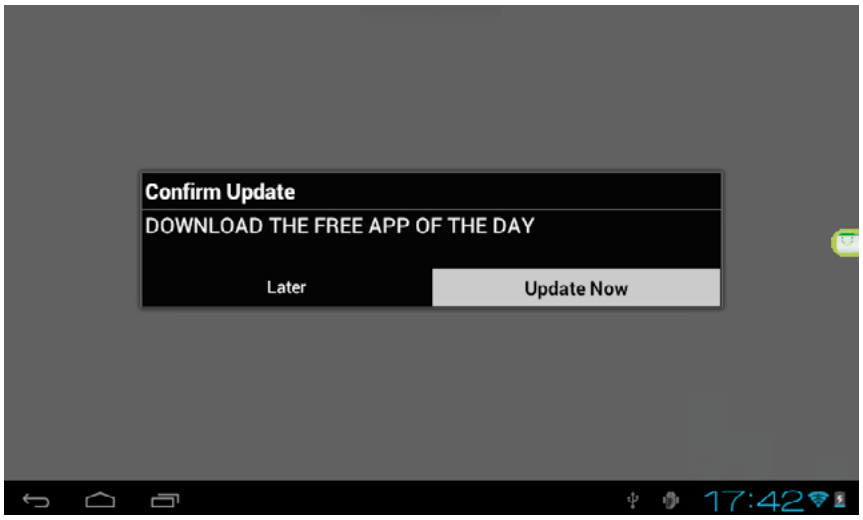
Угрозы в каталоге Google Play

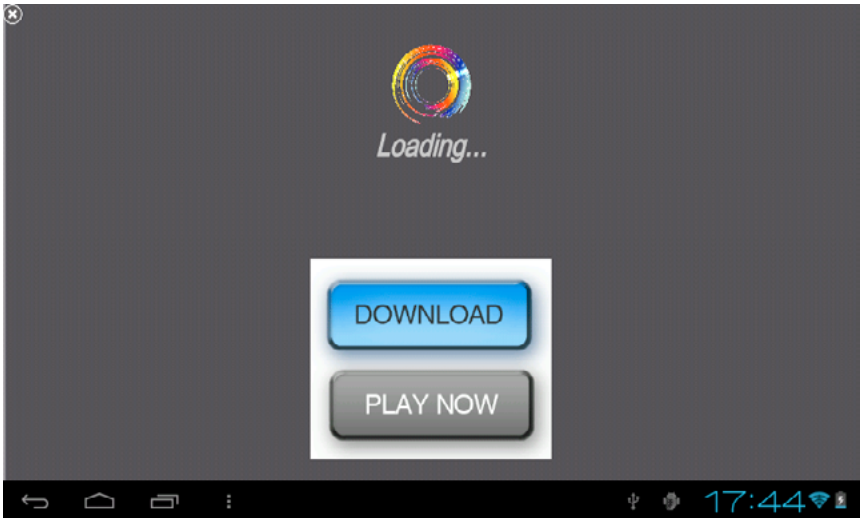
Зачастую размещенные в каталоге Google Play приложения содержат потенциально опасные или нежелательные модули монетизации, которые работают весьма агрессивно, демонстрируя пользователям навязчивую рекламу. В январе был обнаружен очередной такой модуль, который был применен разработчиками ряда бесплатных программ и внесен в вирусную базу Dr.Web под именем **Adware.HideIcon.1.origin.**

Adware.HideIcon.1.origin
Рекламный плагин для монетизации бесплатных Android-приложений. Обладает весьма неприятным функционалом.

- **Может имитировать процесс загрузки важных файлов, обманом заставляя владельца смартфона или планшета перейти на «проплаченный» веб-сайт.**
- С определенной периодичностью предлагает пользователям установить некие «обновления», которые в действительности являются очередными рекламными предложениями.
- Отображает на экране назойливую рекламу при запуске ряда установленных на мобильном устройстве приложений.
- Удаляет оригинальные ярлыки содержащих его программ, в результате чего для неопытных пользователей становится значительно сложнее определить источник столь навязчивых коммерческих предложений. При этом вместо исходных «значков» на главном экране операционной системы создаются новые ярлыки, которые также ведут на различные рекламные предложения в сети Интернет.

Обзор вирусной активности для мобильных Android-устройств за январь 2015 года





Обзор вирусной активности для мобильных Android-устройств за январь 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