Dr.WEB®
с 1992 года

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

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

4 марта 2015 года

Главные тенденции февраля

- Появление новых версий опасных троянцев-вымогателей, шифрующих файлы на мобильных Android-устройствах
- Рост числа агрессивных рекламных модулей, используемых разработчиками ПО для монетизации
- Увеличение количества СМС-троянцев
- Распространение новых троянцев-банкеров

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

Январь 2015	Февраль 2015	Динамика
6087	6665	+9,5%

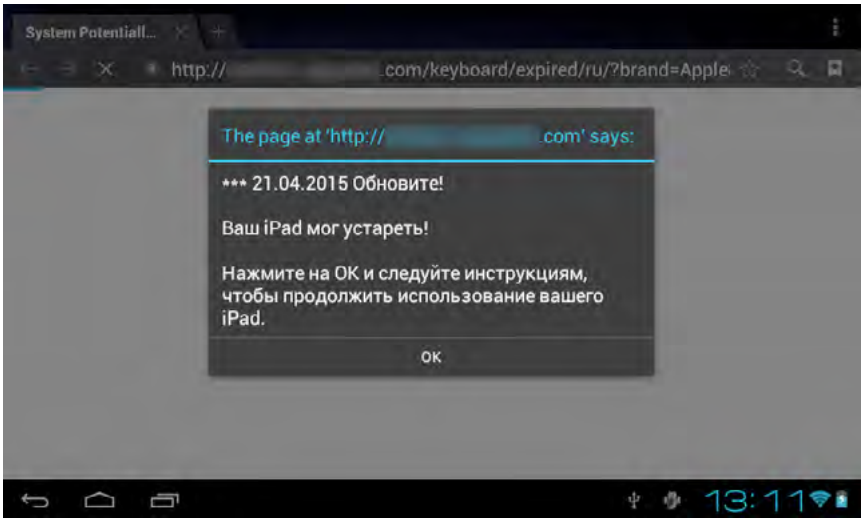
Обзор вирусной активности для мобильных Android-устройств за февраль 2015 года

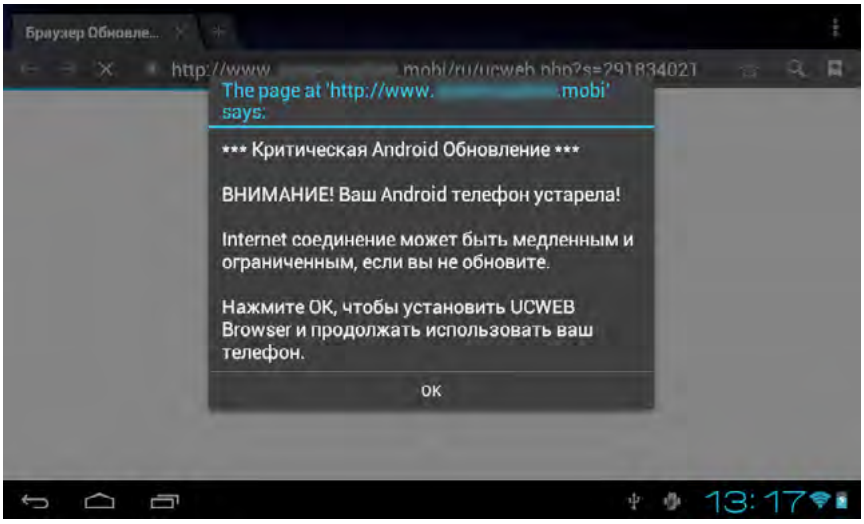
«Мобильная» угроза месяца

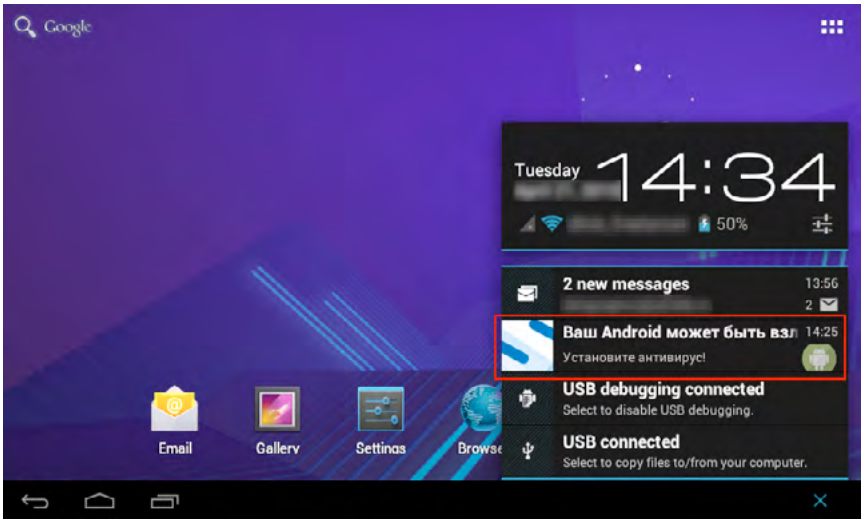
В начале февраля в каталоге цифрового контента Google Play был обнаружен ряд приложений, которые содержали новый агрессивный рекламный модуль **Adware.MobiDash.1.origin**. Некоторые из этих программ были загружены пользователями десятки миллионов раз. **Adware.MobiDash.1.origin** обладает следующими особенностями:

- Может входить в состав самых разнообразных игр и программ, размещенных как в Google Play – официальном каталоге приложений ОС Android, – так и на других популярных онлайн-площадках.
- При каждом выходе Android-устройства из режима ожидания (разблокировки экрана) загружает в веб-браузере интернет-страницы с разнообразной рекламой, а также сомнительными сообщениями, включающими предупреждения о якобы имеющих место неполадках, предложениями установить обновления или определенные программы и т. п.
- Способен отображать рекламу поверх интерфейса операционной системы и пользовательских программ, затрудняя работу с устройством, а также демонстрировать рекламные и иные сообщения в панели уведомлений.
- Прежде чем данный модуль начнет свою активность, должно пройти достаточно длительное время с момента установки и запуска содержащего его приложения. Из-за этого в дальнейшем снижается вероятность обнаружения пользователем источника навязчивой рекламы.

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







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

Агрессивные рекламные модули

В прошедшем месяце специалисты компании «Доктор Веб» отметили появление сразу нескольких новых рекламных систем, обладающих весьма агрессивным функционалом. Одной из них стала платформа Adware.MobiDash.1.origin, которая входила в состав ряда размещенных в каталоге Google Play программ.

Другие «неприятные» рекламные системы:

Adware.HiddenAds.1

- Может устанавливаться на мобильное устройство при помощи различных вредоносных приложений
- Не имеет ярлыка и графического интерфейса, работает в скрытом режиме
- Отображает в панели уведомлений различные рекламные сообщения

Adware.Adstoken.1.origin

- Внедряется третьими лицами в модифицированные и распространяемые ими популярные программы
- Отображает рекламный баннер на экране мобильных устройств
- Демонстрирует различные сообщения в панели уведомлений
- Открывает в веб-браузере сайты с рекламой

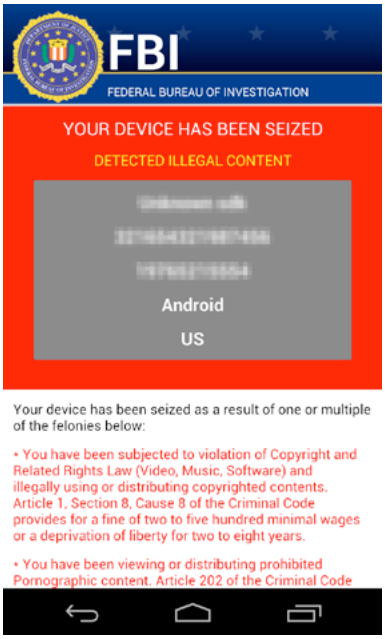
Троянцы-вымогатели

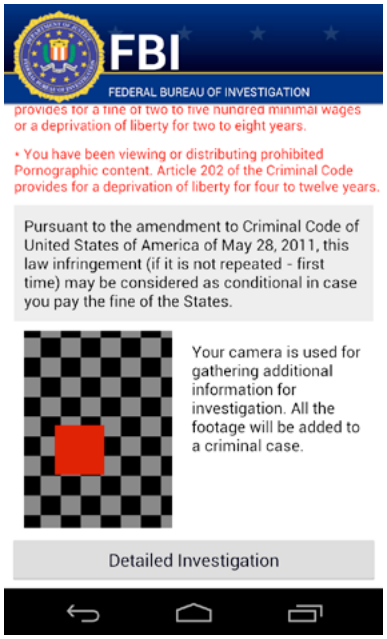
Число записей для троянцев-вымогателей семейства **Android.Locker** в вирусной базе **Dr.Web**:

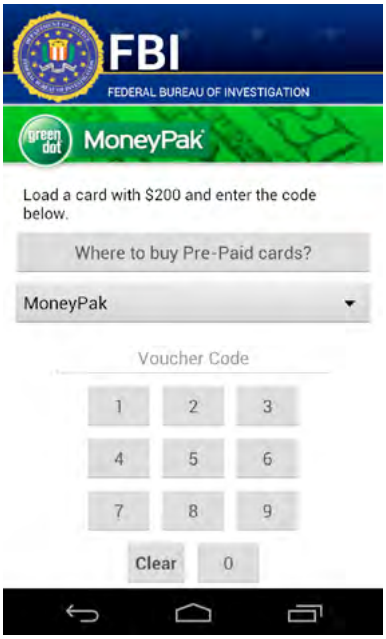
Январь 2015	Февраль 2015	Динамика
159	174	+9,4%

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

В феврале была обнаружена новая модификация опасного троянца-блокировщика **Android.Locker.71.origin**, который шифрует файлы, блокирует зараженные мобильные устройства и требует у пострадавших пользователей выкуп в размере $200.







Шифрование файлов на каждом устройстве происходит с использованием уникального криптографического ключа, поэтому восстановление поврежденных троянцем **Android.Locker.71.origin** данных затруднено.

В настоящий момент расшифровка файлов, пострадавших от действия данной вредоносной программы, невозможна,

однако наши пользователи надежно защищены от действий **Android.Locker.71.origin**, т. к. все известие модификации троянца успешно детектируются и удаляются с мобильных устройств антивирусными решениями Dr.Web для Android.

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

СМС-троянцы

В прошедшем месяце значительно возросло количество новых СМС-троянцев, отправляющих дорогостоящие короткие сообщения и подписывающие мобильные номера жертв на платные услуги. Число записей для троянцев семейства **Android.SmsSend** в вирусной базе Dr.Web:

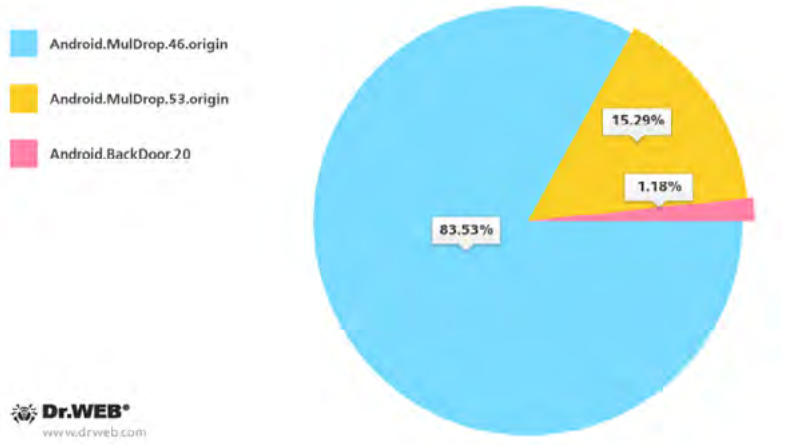
Январь 2015	Февраль 2015	Динамика
2870	3264	+13,7%

Банковские троянцы

В феврале в очередной раз проявили активность всевозможные «мобильные» банковские троянцы. В частности, подобные вредоносные приложения распространялись среди южнокорейских пользователей, где злоумышленники вновь применяли СМС-рассылку сообщений, в которых содержалась ссылка на загрузку копии троянцев.

Выявлено более 80 подобных спам-кампаний, в которых было задействовано несколько вредоносных программ. Большинство из них – троянцы-дропперы.

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



Троянцы Android.MulDrop

Скрывают непосредственно внутри себя других троянцев, в данном случае – Android-банкеров – основной инструментарий южнокорейских вирусописателей.

Android.BackDoor.20

Вредоносная программа, позволяющая злоумышленникам выполнять на зараженных мобильных устройствах различные действия.

Примененные южнокорейскими киберпреступниками троянцы-банкеры:

- Android.BankBot.39.origin
- Android.BankBot.47.origin
- Android.BankBot.48.origin

Все они позволяют получить вирусописателям доступ к банковским счетам пользователей.

Обзор вирусной активности для мобильных Android-устройств за февраль 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

© ООО «Доктор Веб»,
2003-2015