Dr.WEB®
с 1992 года

«Доктор Веб»: обзор вирусной активности для мобильных Android-устройств в июле 2015 года

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

3 августа 2015 года

Главные тенденции июля

- Использование злоумышленниками различных рекламных модулей для монетизации троянских программ
- Появление новых вредоносных приложений в каталоге Google Play
- Появление опасных троянцев-бэкдоров
- Рост числа Android-вымогателей
- Увеличение числа СМС-троянцев

Количество записей для вредоносных и нежелательных программ под ОС Android в вирусной базе Dr.Webдля внедрения в веб-страницы посторонней рекламы.

Июнь 2015	Июль 2015	Динамика
10 144	11 422	+12,6%

«Мобильная» угроза месяца

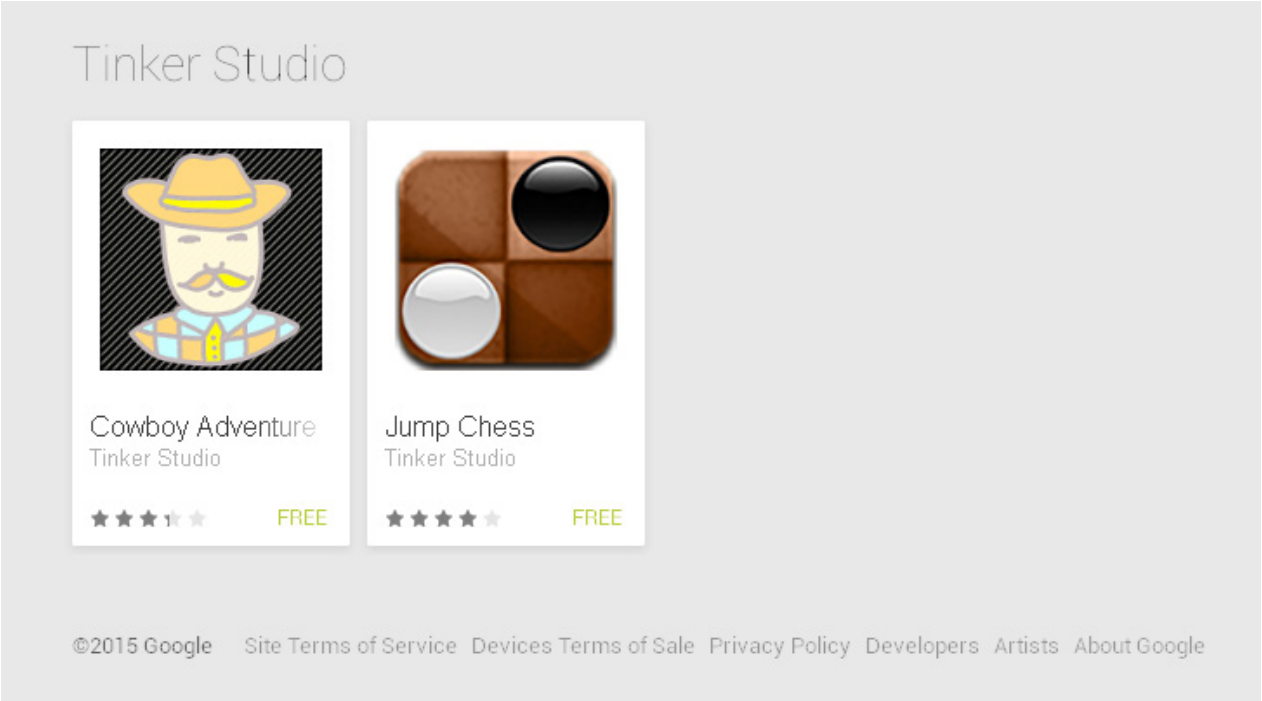
В июле был обнаружен весьма примечательный Android-троянец, добавленный в вирусную базу Dr.Web как **Android.Poder.1**. Это вредоносное приложение, внедренное злоумышленниками в целый ряд безобидных программ (преимущественно игр), осуществляет кражу конфиденциальных данных, может рассылать по всем контактам из телефонной книги пользователя СМС-сообщения со ссылкой на загрузку копии троянца, а также демонстрирует различные рекламные сообщения, принося прибыль своим создателям. Помимо показа рекламы, **Android.Poder.1** обладает еще одним инструментом монетизации. В частности, для доступа к некоторым функциям, которые в оригинальных приложениях были бесплатными, пользователям предлагается совершить небольшой платеж, который в итоге поступает предприимчивым вирусописателям. Особенности данного троянца:

- встроен в целый ряд игровых приложений, модифицированных злоумышленниками;
- выполняет сбор конфиденциальной информации, такой как история посещения сайтов в веб-браузере и сохраненные закладки;
- способен отправлять на номера из телефонной книги пользователя СМС-сообщения со ссылкой на загрузку копии троянца (в зависимости от модификации вредоносного приложения отправка может осуществляться без ведома владельца мобильного устройства, либо с его согласия – в этом случае используется стандартная форма отправки сообщений);
- содержит несколько программных модулей, предназначенных для показа назойливой рекламы;
- может предлагать пользователям оплатить доступ к некоторым функциям скомпрометированного злоумышленниками приложения.

Android-троянцы в Google Play

В прошедшем июле специалисты по информационной безопасности выявили очередных Android-троянцев, которые были загружены вирусописателями в каталог Google Play. Данные вредоносные программы получили по классификации компании «Доктор Веб» имена Android.Spy.134 и Android.Spy.135 и скрывались в безобидных, на первый взгляд, играх. Эти троянцы были способны демонстрировать на экране поддельное окно аутентификации приложения-клиента Facebook, запрашивая у владельцев мобильных устройств логин и пароль от их учетных записей, и передавали введенные данные на удаленный сервер. Вскоре после этого многие пользователи социальной сети, находящиеся в списке контактов жертв, могли получить сообщение от «друга», в котором рекомендовалось установить игру, перейдя по указанной ссылке. Благодаря такому

приему создатели троянцев добились значительных успехов в их распространении: на момент удаления Android.Spy.134 и Android.Spy.135 из каталога Google Play в общей сложности они были загружены более 500 000 раз.



Особенности данных троянцев:

- более 500 000 загрузок в каталоге Google Play;
- созданы с использованием программной платформы Mono Framework;
- для установивших данные вредоносные программы пользователей троянцы выглядят как полноценные игры;
- были способны демонстрировать поддельное окно аутентификации приложения-клиента Facebook, запрашивая у жертв логин и пароль от их учетных записей;
- могли распространять среди «друзей» из списка контактов пользователей социальной сети Facebook сообщение с рекомендацией установить игру, перейдя по указанной ссылке.

В конце июля вирусные аналитики «Доктор Веб» обнаружили в каталоге Google Play другого троянца, получившего имя Android.DownLoader.171.origin. Это вредоносное приложение предназначено для загрузки и установки различных программ на мобильные

устройства. Кроме того, по команде вирусописателей оно способно удалять уже установленное ПО. Еще одной вредоносной функцией Android.DownLoader.171.origin является демонстрация рекламы в панели нотификаций операционной системы.

На момент обнаружения этого троянца в каталоге Google Play его успели скачать более 100 000 пользователей. Однако злоумышленники распространяли данное приложение и на других популярных онлайн-площадках, ориентированных, преимущественно, на китайскую аудиторию. В результате общее число установивших Android.DownLoader.171.origin владельцев Android-устройств превысило 1,5 миллиона. Подробнее о троянце рассказано в опубликованном материале на сайте компании «Доктор Веб».

Троянцы-бэкдоры

В минувшем месяце вирусная база Dr.Web пополнилась сразу несколькими новыми записями для троянцев-бэкдоров семейства Android.Backdoor, предназначенных для выполнения на зараженных мобильных устройствах различных нежелательных действий по команде вирусописателей. В частности, среди выявленных вредоносных программ такого типа стоит отметить троянцев Android.Backdoor.114.origin и Android.Backdoor.213.origin. Данные бэкдоры распространялись вирусописателями в модифицированных ими безобидных приложениях и были способны красть у пользователей различную конфиденциальную информацию, а также незаметно загружать и устанавливать другие приложения. Ко всему прочему, троянец Android.Backdoor.114.origin пытался получить root-доступ в инфицированной системе для того, чтобы выполнить свою установку в системный каталог, обеспечив себе тем самым определенную защиту от своего удаления.

Число записей для троянцев семейства Android.Backdoor в вирусной базе Dr.Web:

Июнь 2015	Июль 2015	Динамика
214	257	+20,1%

Android-вымогатели

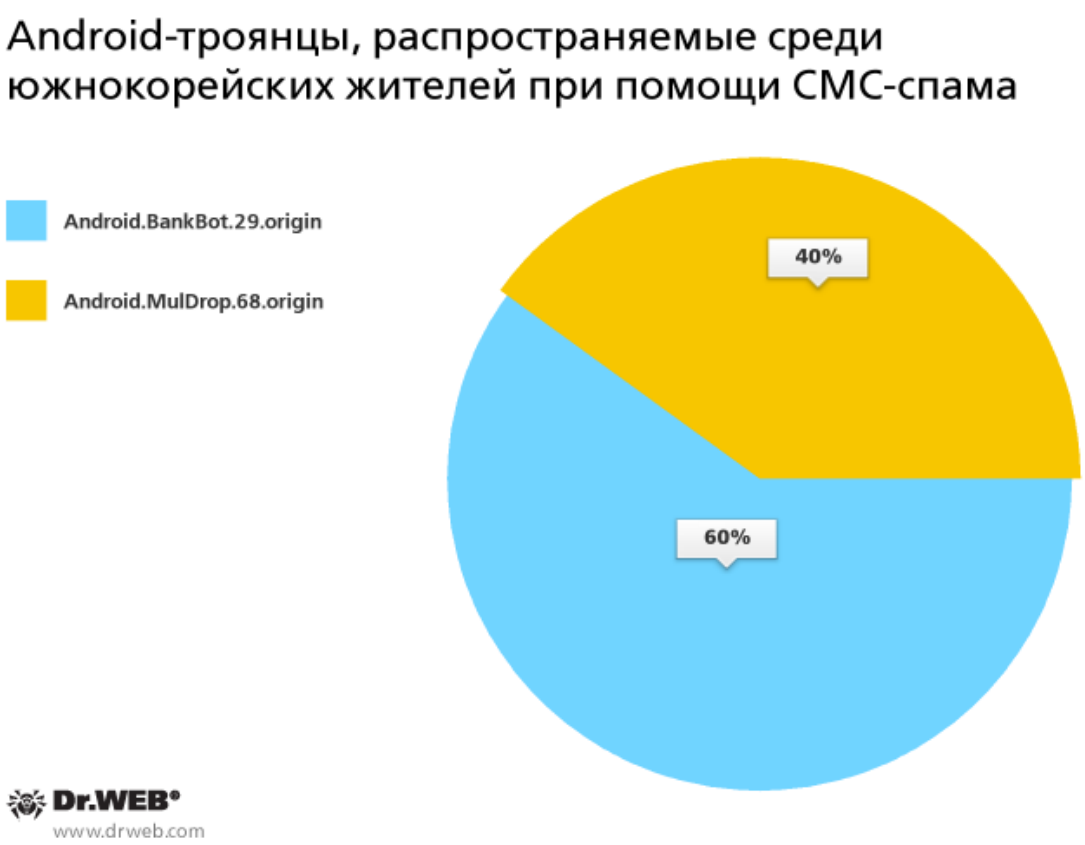
В июле было выявлено большое число новых троянцев-вымогателей семейства Android.Locker. Эти опасные вредоносные приложения блокируют мобильные устройства и требуют у пользователей выкуп за их разблокировку. Число записей для Android-вымогателей в вирусной базе Dr.Web:

Июнь 2015	Июль 2015	Динамика
301	356	+14,8%

Банковские троянцы

В июле злоумышленники продолжили распространять всевозможных троянцев, предназначенных для кражи денег с банковских счетов. Так, южнокорейские вирусописатели вновь организовали несколько спам-кампаний по рассылке СМС-сообщений, в которых указывалась ссылка на загрузку копии того или иного вредоносного Android-приложения. По сравнению с предыдущими месяцами, число таких атак было невелико и составило менее десятка.

При этом в июле киберпреступники из Южной Кореи при помощи СМС-спама распространяли следующих Android-троянцев:



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

Июнь 2015	Июль 2015	Динамика
122	135	+10,65%

- 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.68.origin

Троянец, предназначенный для распространения и установки на мобильные устройства других вредоносных приложений.

СМС-троянцы

Также в прошедшем месяце было обнаружено большое число новых СМС-троянцев, отправляющих дорогостоящие сообщения на премиум-номера и подписывающих пользователей на ненужные платные услуги. Число записей для СМС-троянцев Android.SmsSend в вирусной базе Dr.Web:

Июнь 2015	Июль 2015	Динамика
4745	5259	+10,83%

Обзор вирусной активности для мобильных Android-устройств в июле 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