Dr.WEB®
с 1992 года

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

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

30 августа 2015 года

Главные тенденции августа

- Новые атаки с использованием банкеров
- Применение Android-троянцев для кибершпионажа
- Рост числа Android-вымогателей
- Увеличение числа СМС-троянцев

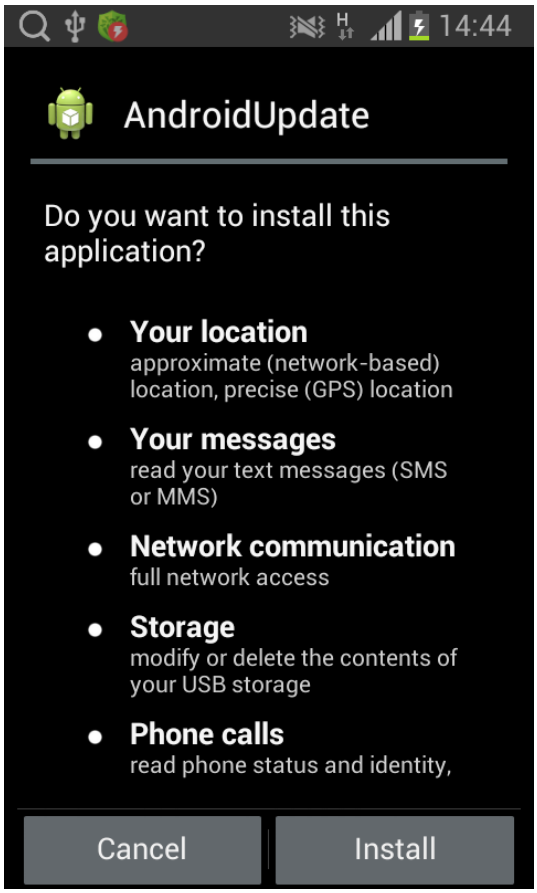
Количество записей для вредоносных и нежелательных программ под ОС Android в вирусной базе Dr.Web

Июль 2015	Август 2015	Динамика
11 422	12 504	+9,47%

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

«Мобильная» угроза месяца

В августе специалисты компании «Доктор Веб» исследовали образец нового Android-троянца, созданного злоумышленниками для кибершпионажа. Эта вредоносная программа, получившая имя Android.Backdoor.260.origin, предназначена для слежки за китайскими пользователями и способна перехватывать СМС-сообщения, переписку в мессенджере QQ, красть информацию из телефонной книги, незаметно производить аудиозапись окружения с использованием встроенного микрофона, получать координаты зараженного мобильного устройства и перехватывать все вводимые жертвой данные.



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

Особенности Android.Backdoor.260.origin:

- устанавливается на мобильные устройства под видом некоего обновления;
- после запуска удаляет свой ярлык, «прячась» от пользователя;
- пытается поместить несколько троянских модулей в системные каталоги;
- взаимодействие вредоносных модулей осуществляется через сокеты UNIX;
- пытается незаметно установить потенциально опасную утилиту, позволяющую ему отслеживать вводимые жертвой данные;
- может управляться злоумышленниками дистанционно.

Более подробная информация об этом вредоносном приложении содержится в опубликованном специалистами компании «Доктор Веб» материале.

Банковские троянцы

В августе пользователи мобильных Android-устройств вновь оказались под прицелом киберпреступников, охотившихся за деньгами на банковских счетах, однако активность таких злоумышленников была заметно ниже, чем в предыдущие месяцы. Как и прежде, вирусописатели использовали свой излюбленный способ распространения банковских троянцев, а именно – применяли спам-рассылку СМС-сообщений, в которых указывали ведущую на загрузку вредоносного приложения ссылку.

Так, среди южнокорейских пользователей Android распространялся троянец Android.MulDrop.69.origin, устанавливающий на мобильные устройства вредоносную программу Android.MulDrop.38, которая, в свою очередь, инсталлировала банкера Android.BankBot.74.origin.

В то же время при атаках на российских пользователей были замечены банковские троянцы Android.SmsBot.365.origin, а также Android.SmsBot.451.origin, которых вирусописатели распространяли под видом поступивших MMS-сообщений.

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

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

Июль 2015	Август 2015	Динамика
135	138	+2,22%

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

Июль 2015	Август 2015	Динамика
473	495	+4,65%

Android.MulDrop.46.origin

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

Android.MulDrop.38

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

Android.BankBot.74.origin

Троянец, предназначенный для кражи денег с банковских счетов пользователей мобильных устройств под управлением ОС Android.

Android.SmsBot.365.origin

Троянец, предназначенный для кражи денег с банковских счетов пользователей мобильных устройств под управлением ОС Android.

Android.SmsBot.451.origin

Троянец, предназначенный для кражи денег с банковских счетов пользователей мобильных устройств под управлением ОС Android.

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

Android-вымогатели

В прошедшем месяце вирусные аналитики компании «Доктор Веб» вновь отметили заметный рост числа опасных троянцев-вымогателей семейства Android.Locker, которые блокируют мобильные устройства и требуют выкуп за их разблокировку. Число записей для Android-вымогателей в вирусной базе Dr.Web:

Июль 2015	Август 2015	Динамика
356	431	+21%

СМС-троянцы

В августе увеличилось количество 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:

Июль 2015	Август 2015	Динамика
5259	5728	+9%

Обзор вирусной активности для мобильных Android-устройств в августе 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