Dr.WEB®
с 1992 года

Обзор вирусной активности для мобильных Android-устройств в сентябре 2017 года

Обзор вирусной активности для мобильных Android-устройств в сентябре 2017 года

29 сентября 2017 года

В сентябре широкую известность получила группа уязвимостей BlueBorne в стеке протокола Bluetooth, которую выявили специалисты по информационной безопасности. Эти уязвимости позволяют злоумышленникам получить полный контроль над Bluetooth-совместимыми устройствами, распространять среди них вредоносные программы и незаметно красть конфиденциальную информацию. Кроме того, в прошедшем месяце в каталоге Google Play был найден очередной банковский троянец.

Главные тенденции сентября

- Появление информации об опасных уязвимостях в реализации протокола Bluetooth, которым подвержены многие устройства, включая Android-смартфоны и планшеты;
- Обнаружение в Google Play банковского троянца, встроенного в безобидную игру.

Обзор вирусной активности для мобильных Android-устройств в сентябре 2017 года

«Мобильная» угроза месяца

В сентябре стало известно об обнаружении целого ряда уязвимостей в стеке протокола Bluetooth, получивших название BlueBorne. Они позволяют злоумышленникам полностью контролировать широкий спектр атакуемых устройств, выполнять на них произвольный код и красть конфиденциальную информацию. Опасности подвержены в том числе смартфоны и планшеты под управлением Android, на которых не установлены закрывающие эти уязвимости «заплатки» ОС.

Специалисты компании «Доктор Веб» готовят обновление антивируса Dr.Web Security Space для Android, которое позволит наряду с уже известными уязвимостями обнаруживать на защищаемых устройствах и указанные программные ошибки.

Обзор вирусной активности для мобильных Android-устройств в сентябре 2017 года

По данным антивирусных продуктов Dr.Web для Android

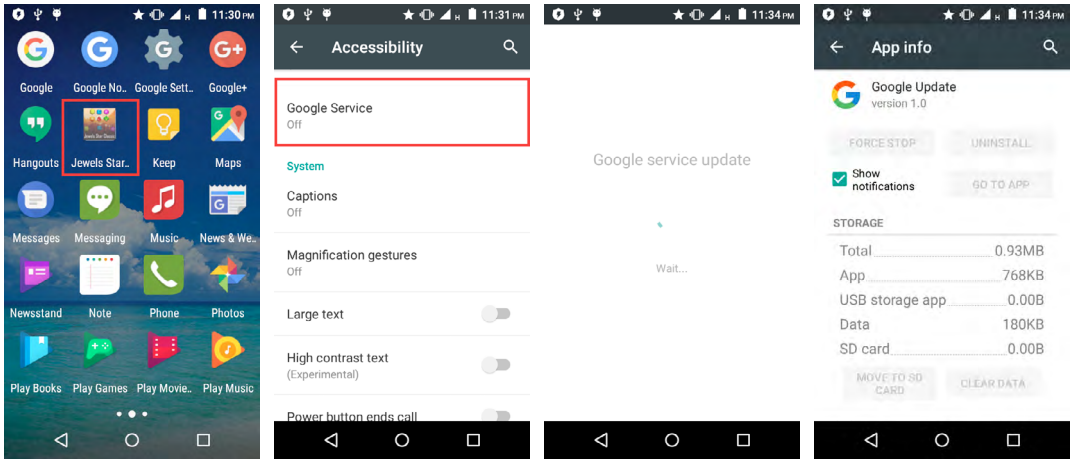
- **Android.Click.171.origin**
  Представитель семейства троянцев, предназначенных для накрутки количества посещений заданных злоумышленниками веб-сайтов.
- **Android.DownLoader.337.origin**
  Троянская программа, предназначенная для загрузки других приложений.
- **Android.CallPay.1.origin**
  Вредоносная программа, которая предоставляет владельцам Android-устройств доступ к эротическим материалам, но в качестве оплаты этой «услуги» незаметно совершает звонки на премиум-номера.
- **Android.HiddenAds.109.origin**
  Троянцы, предназначенные для показа навязчивой рекламы. Распространяются под видом популярных приложений другими вредоносными программами, которые в некоторых случаях незаметно устанавливают их в системный каталог.
- **Android.Triada.152**
  Представитель семейства многофункциональных троянцев, выполняющих разнообразные вредоносные действия.

- **Adware.Jiubang.2**
- **Adware.SalmonAds.1.origin**
- **Adware.Fly2tech.2**
- **Adware.Avazu.8.origin**
- **Adware.Jiubang.1**
  Нежелательные программные модули, встраиваемые в Android-приложения и предназначенные для показа навязчивой рекламы на мобильных устройствах.

Обзор вирусной активности для мобильных Android-устройств в сентябре 2017 года

Троянец в Google Play

В сентябре в каталоге Google Play был выявлен банковский троянец Android.BankBot.234.origin, который скрывался в безобидной игре под названием Jewels Star Classic. Через некоторое время после запуска он запрашивает доступ к функциям специальных возможностей Android. С их помощью вредоносная программа скрытно устанавливает и запускает спрятанный в ее ресурсах троянец Android.BankBot.233.origin. В свою очередь, Android.BankBot.233.origin отслеживает запуск приложения «Play Маркет» и показывает поверх его окна фишинговую форму настройки платежного сервиса, в которой запрашивает информацию о банковской карте. Введенные пользователем сведения передаются вирусописателям, после чего те могут незаметно украсть деньги со счета жертвы, т. к. троянец перехватывает все СМС-сообщения с проверочными кодами.



Особенности Android.BankBot.234.origin:

- встроен в безобидную игру;
- чтобы не вызывать подозрений, начинает вредоносную деятельность спустя некоторое время после установки и запуска;
- пытается получить доступ к Специальным возможностям (Accessibility Service) устройства, с использованием которых может самостоятельно нажимать на кнопки в диалоговых окнах, включать необходимые системные параметры и устанавливать приложения;
- содержит в своих ресурсах троянца Android.BankBot.233.origin, который устанавливается незаметно для владельца зараженного смартфона или планшета и используется для кражи сведений о банковской карте.

Для владельцев Android-устройств опасность представляют не только вредоносные приложения, которые распространяются в Интернете и встречаются даже в официальном каталоге Android-программ Google Play, но и различные уязвимости операционной системы и ее компонентов. Для защиты от этих угроз необходимо своевременно устанавливать все доступные обновления, а также использовать антивирусные продукты Dr.Web для Android.

Обзор вирусной активности для мобильных Android-устройств в сентябре 2017 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
125040, 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