Dr.WEB®
с 1992 года

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

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

31 августа 2017 года

В августе в каталоге Google Play было обнаружено большое число вредоносных Android-приложений, в том числе троянцы, которые выполняли DDoS-атаки. Другие вредоносные программы незаметно загружали указанные злоумышленниками веб-сайты и самостоятельно нажимали на размещенные на них баннеры, за что вирусописатели получали вознаграждение. Еще один Android-троянец, выявленный в Google Play в августе, показывал поддельные формы ввода поверх запускаемых программ и похищал логины, пароли и другую конфиденциальную информацию. Кроме того, в последнем летнем месяце в Google Play был найден троянец-дроппер, предназначенный для установки прочих вредоносных приложений.

Главные тенденции августа

- Обнаружение вредоносных Android-программ, выполнявших DDoS-атаки на веб-сайты;
- Выявление в Google Play Android-банкера, который скрывался в безобидном приложении;
- Проникновение в Google Play троянца, предназначенного для установки других вредоносных программ.

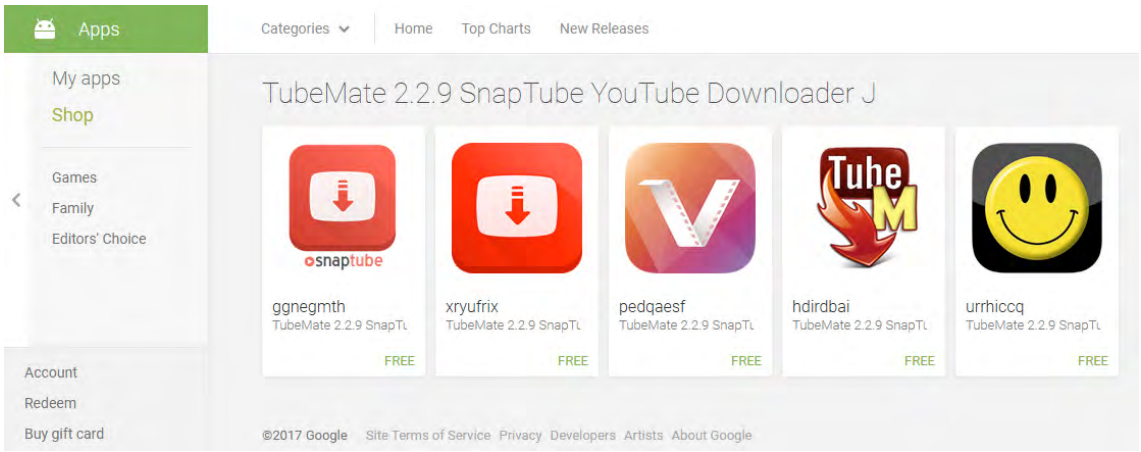
Обзор вирусной активности для мобильных Android-устройств в августе 2017 года

«Мобильная» угроза месяца

В августе в каталоге Google Play было обнаружено несколько троянцев семейства Android.Click. Два из них получили имена Android.Click.268 и Android.Click.274 соответственно. После запуска они незаметно для владельцев мобильных устройств выполняли DDoS-атаки («Отказ в обслуживании») на указанные вирусописателями веб-сайты, открывая несколько их копий, а также могли по команде отправлять множество сетевых пакетов на целевые серверы. В результате пользователи зараженных Android-смартфонов и планшетов, которые загрузили эти программы, невольно становились соучастниками киберпреступлений.

Другой троянец, добавленный в вирусную базу Dr.Web как Android.Click.269, незаметно открывал заданные в командах злоумышленников веб-сайты и нажимал на размещенные на них баннеры. За это авторы вредоносного приложения получали вознаграждение. Помимо этого, Android.Click.269 показывал рекламу при разблокировке экрана зараженных Android-устройств.

Все указанные троянцы были встроены в ПО для просмотра видео с сервиса YouTube.



Особенности Android.Click.268 и Android.Click.274:

- осуществляют DDoS-атаки на сайты, незаметно для пользователя загружая 20 копий заданного злоумышленниками веб-ресурса;
- могут выполнять DDoS-атаки на удаленные хосты по протоколу UDP, отправляя 10 000 000 пакетов на указанный в команде порт сервера.

Особенности AndAndroid.Click.269:

- незаметно открывает указанные в команде вирусописателей веб-сайты и автоматически нажимает на рекламные баннеры, принося авторам троянца прибыль;
- показывает рекламу при разблокировке экрана зараженного мобильного устройства.

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

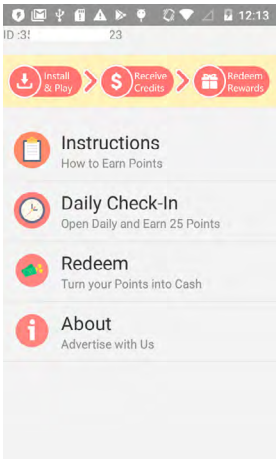
По данным антивирусных продуктов Dr.Web для Android

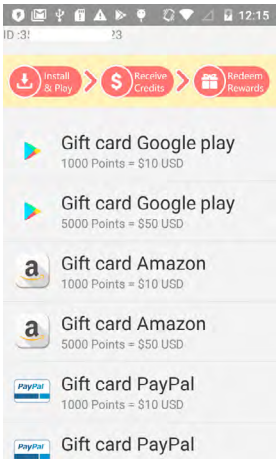
- **Android.DownLoader.337.origin**
- **Android.DownLoader.526.origin**
  Троянские программы, предназначенные для загрузки других приложений.
- **Android.CallPay.1.origin**
  Вредоносная программа, которая предоставляет владельцам Android-устройств доступ к эротическим материалам, но в качестве оплаты этой «услуги» незаметно совершает звонки на премиум-номера.
- **Android.HiddenAds.85.origin**
- **Android.HiddenAds.83.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.

- **Adware.Jiubang.2**
- **Adware.Fly2tech.2**
- **Adware.SalmonAds.1.origin**
- **Adware.Jiubang.1**
- **Adware.Batmobi.4**
  Нежелательные программные модули, встраиваемые в Android-приложения и предназначенные для показа навязчивой рекламы на мобильных устройствах.

Троянец в Google Play

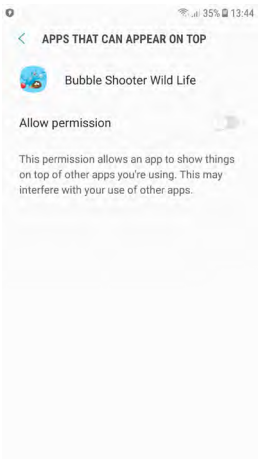
В последнем летнем месяце в вирусную базу Dr.Web был добавлен банковский троянец Android.BankBot.225.origin, который распространялся через каталог Google Play. Он был скрыт внутри приложения под названием «Earn Real Money Gift Cards», предназначенного для получения подарочных денежных сертификатов за установку рекламируемых программ.

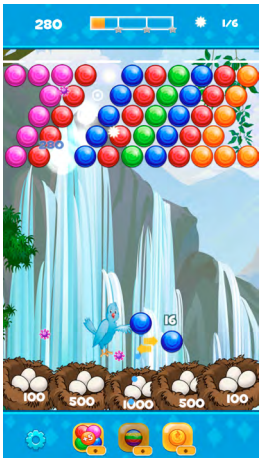




Android.BankBot.225.origin отслеживает запуск банковских и других приложений и показывает поверх их окон поддельные формы ввода конфиденциальной информации. Кроме того, по команде вирусописателей он может скачивать на зараженные устройства прочие программы, которые затем пытается установить.

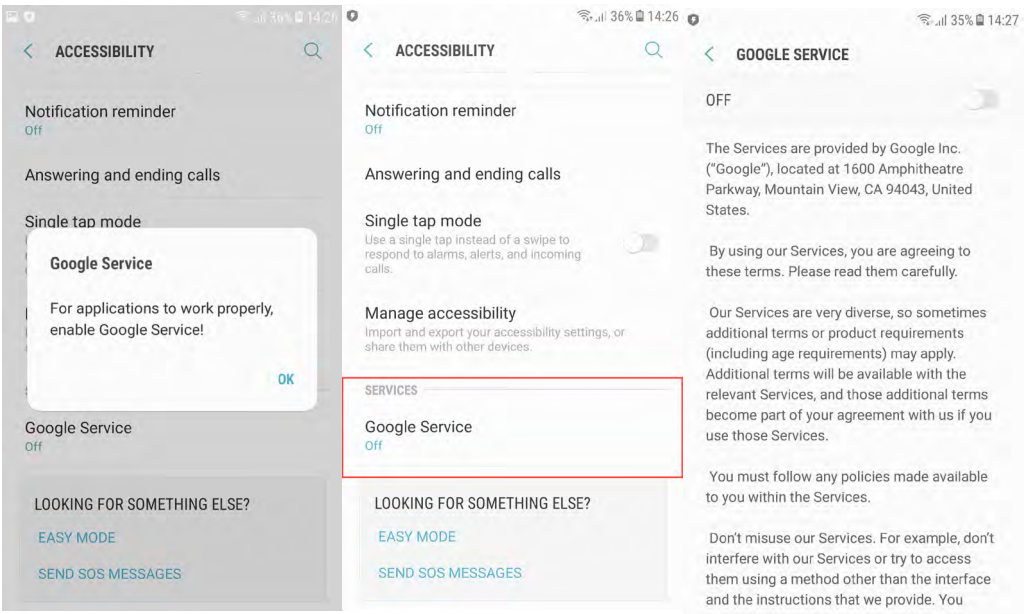
Еще один троянец, обнаруженный в Google Play в августе, был внесен в вирусную базу Dr.Web как Android.MulDrop.1067. Он скрывался в игре под названием «Bubble Shooter Wild Life». При каждом старте эта вредоносная программа запрашивает разрешение на отображение элементов интерфейса поверх других приложений.





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

Через некоторое время после запуска она пытается получить доступ к специальным возможностям (Accessibility Service), показывая соответствующее уведомление. Если владелец устройства соглашается предоставить троянцу нужные полномочия, Android.MulDrop.1067 может самостоятельно устанавливать другие Android-приложения, автоматически нажимая на кнопки в диалоговых окнах и подтверждая все действия. Троянец проверяет наличие на карте памяти apk-файла, который он должен установить, однако текущая версия Android.MulDrop.1067 не содержит никаких скрытых файлов и не имеет функции загрузки их из Интернета. Это может говорить о том, что троянец все еще находится на стадии разработки.



Вирусописатели всеми способами пытаются распространять Android-троянцев через каталог приложений Google Play. Чтобы увеличить вероятность заражения мобильных устройств, они встраивают вредоносные программы в полнофункциональные приложения и используют различные механизмы обхода проверки безопасности, чтобы троянцы как можно дольше оставались незамеченными. Для защиты смартфонов и планшетов под управлением ОС Android пользователям необходимо установить антивирусные продукты Dr.Web, которые способны бороться с современными Android-угрозами.

Обзор вирусной активности для мобильных Android-устройств в августе 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