Dr.WEB®
с 1992 года

«Доктор Веб»: обзор вирусной активности для мобильных устройств в октябре 2018 года

Обзор вирусной активности для мобильных устройств в октябре 2018 года

31 октября 2018 года

В октябре специалисты по информационной безопасности обнаружили Android-троянца, способного выполнять полученные с удаленного сервера скрипты, написанные на языке C#, а также скачивать и запускать вредоносные модули. Кроме того, в течение уходящего месяца в каталоге Google Play были вновь выявлены вредоносные приложения.

Главные тенденции октября

- Обнаружение вредоносных программ в каталоге Google Play
- Выявление Android-троянца, который мог получать от злоумышленников и компилировать C#-код непосредственно перед его выполнением на мобильных устройствах

Обзор вирусной активности для мобильных устройств в октябре 2018 года

Мобильная угроза месяца

В октябре специалисты компании «Доктор Веб» обнаружили в каталоге Google Play троянца-загрузчика Android.DownLoader.818.origin, распространявшегося под видом VPN-клиента. Вредоносная программа скачивала на мобильные устройства и пыталась установить рекламного троянца. Позже вирусные аналитики выявили модификации этого загрузчика, которые получили имена Android.DownLoader.819.origin и Android.DownLoader.828.origin. Злоумышленники выдавали их за различные игры.

Особенности троянцев:

- пытаются получить права администратора мобильного устройства, чтобы затруднить свое удаление;
- скрывают значок приложения из списка установленных программ главного экрана операционной системы;
- загружают и предлагают пользователю установить других троянцев, которые маскируются под системное ПО.

Обзор вирусной активности для мобильных устройств в октябре 2018 года

По данным антивирусных продуктов Dr.Web для Android

Android.Backdoor.682.origin

Android.Backdoor.1521

Троянские программы, которые выполняют команды злоумышленников и позволяют им контролировать зараженные мобильные устройства.

Android.HiddenAds.261.origin

Android.HiddenAds.288.origin

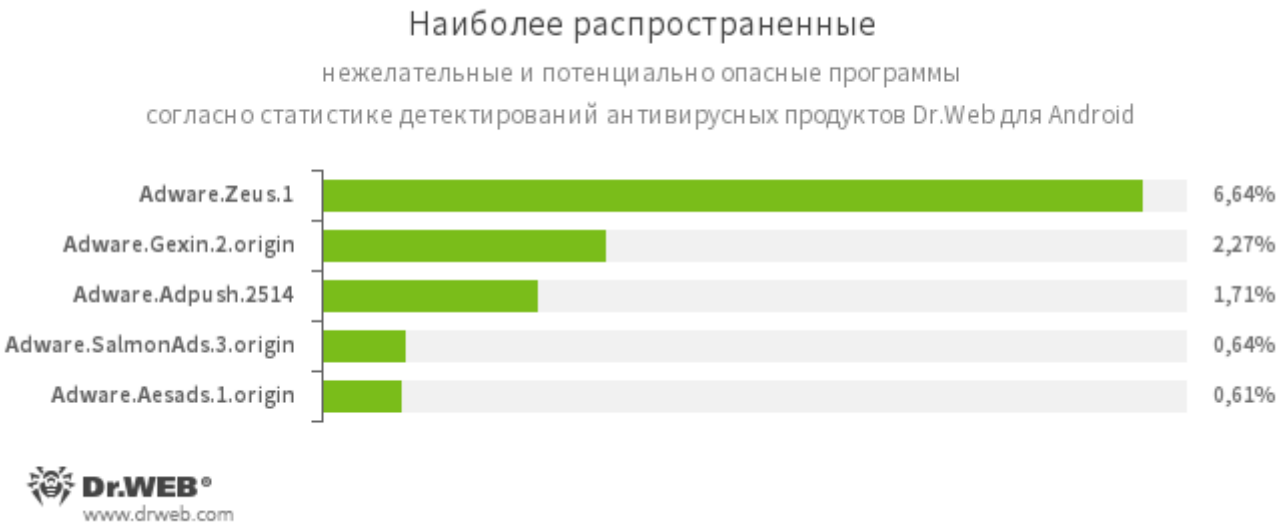
Троянцы, предназначенные для показа навязчивой рекламы. Распространяются под видом популярных приложений другими вредоносными программами, которые в некоторых случаях незаметно устанавливают их в системный каталог.

Android.DownLoader.573.origin

Троянец, загружающий другие вредоносные приложения.

Обзор вирусной активности для мобильных устройств в октябре 2018 года

По данным антивирусных продуктов Dr.Web для Android



Adware.Zeus.1

Adware.Gexin.2.origin

Adware.Adpush.2514

Adware.SalmonAds.3.origin

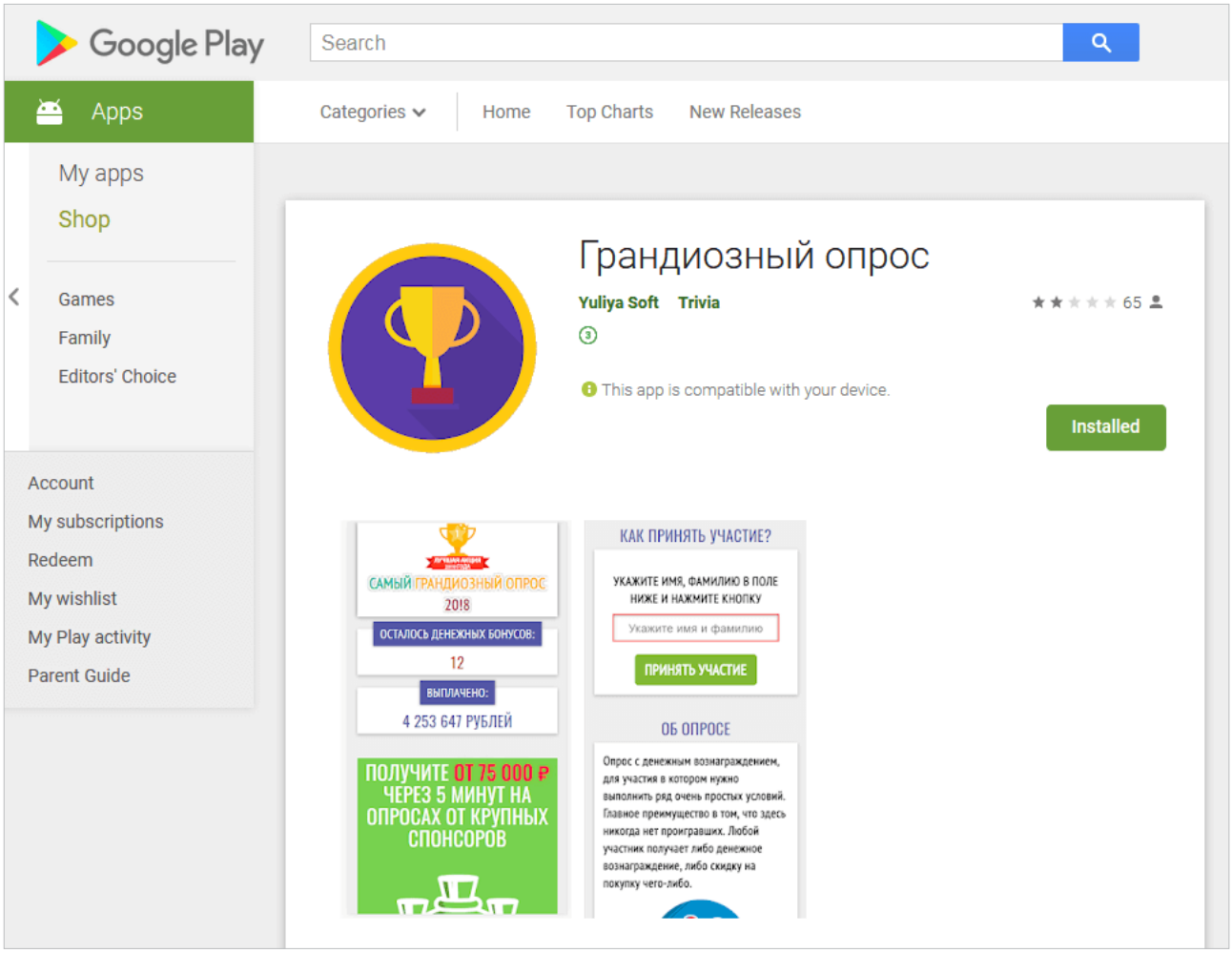
Adware.Aesads.1.origin

Нежелательные программные модули, встраиваемые в Android-приложения и предназначенные для показа навязчивой рекламы на мобильных устройствах.

Обзор вирусной активности для мобильных устройств в октябре 2018 года

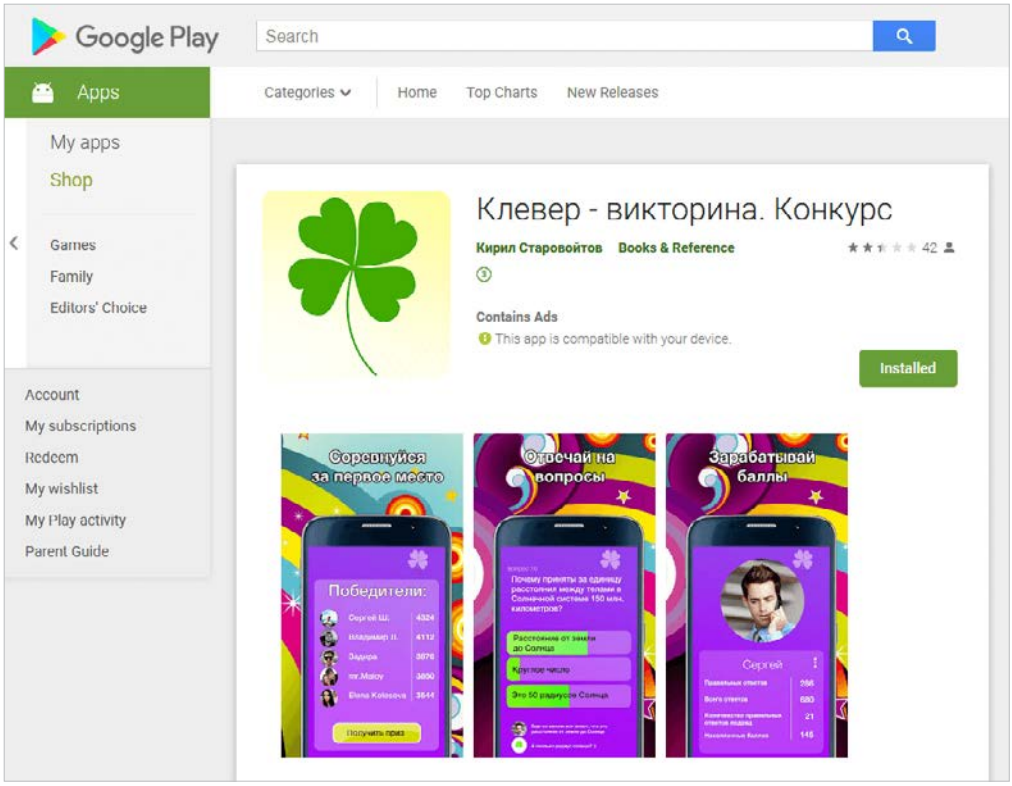
Трояны в Google Play

В начале месяца специалисты «Доктор Веб» обнаружили в каталоге Google Play трояна Android.FakeApp.125. Он распространялся под видом программы, с помощью которой пользователи якобы могли заработать деньги, отвечая на простые вопросы. В действительности же Android.FakeApp.125 по команде управляющего сервера загружал и показывал потенциальным жертвам мошеннические веб-сайты.



Позже вирусные аналитики выявили трояна Android.Click.245.origin, которого киберпреступники выдавали за популярную игру «Клевер», принадлежащую социальной сети «ВКонтакте». Как и Android.FakeApp.125, Android.Click.245.origin загружал страницы мошеннических веб-порталов и демонстрировал их пользователям.

Троянцы в Google Play



В конце октября аналитики «Доктор Веб» исследовали вредоносные программы Android.RemoteCode.192.origin и Android.RemoteCode.193.origin. Они скрывались в 18 безобидных, на первый взгляд, программах — сканерах штрих-кодов, ПО для навигации, менеджерах загрузок файлов и различных играх, которые в общей сложности установили как минимум 1 600 000 владельцев Android-смартфонов и планшетов. Эти троянцы показывали рекламу, могли скачивать и запускать вредоносные модули, а также открывать заданные злоумышленниками видео на портале YouTube, искусственно увеличивая их популярность.

Помимо этого, в вирусную базу Dr.Web были добавлены записи для детектирования вредоносных программ Android.DownLoader.3897, Android.DownLoader.826.origin и Android.BankBot.484.origin. Они загружали на мобильные устройства и пытались установить банковских троянцев.

Прочие угрозы

Среди обнаруженных в октябре вредоносных программ для мобильных устройств оказался Android-банкер Android.BankBot.1781, имеющий модульную архитектуру. По команде управляющего сервера он мог загружать различные троянские плагины, а также скачивать и выполнять написанные на языке C# скрипты. Android.BankBot.1781 похищал информацию о банковских картах, мог красть СМС-сообщения и другую конфиденциальную информацию.

Злоумышленники распространяют вредоносные программы для мобильных Android-устройств как через каталог приложений Google Play, так и с применением мошеннических или взломанных веб-сайтов. Для защиты смартфонов и планшетов пользователям следует установить антивирусные продукты Dr.Web для Android.

Обзор вирусной активности для мобильных устройств в октябре 2018 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 | free.drweb.ru | www.av-desk.ru
«Доктор Веб» в других странах