Dr.WEB®
с 1992 года

«Доктор Веб»: обзор вирусной активности для мобильных устройств в ноябре 2020 года

«Доктор Веб»: обзор вирусной активности для мобильных устройств в ноябре 2020 года

16 декабря 2020 года

В ноябре антивирусные продукты Dr.Web для Android выявили на защищаемых устройствах на 5,14% меньше угроз по сравнению с октябрем. Согласно статистике детектирований, число обнаруженных вредоносных программ снизилось на 8,37%. В то же время число нежелательных, потенциально опасных и рекламных программ, наоборот, увеличилось на 5,78%, 13,16% и 5,72% соответственно.

Среди угроз, выявленных в каталоге Google Play вирусными аналитиками «Доктор Веб», оказался троян Android.Mixi.44.origin. Он загружал и показывал сайты поверх окон других приложений, незаметно переходил по ссылкам и позволял злоумышленникам зарабатывать на том, что пользователи устанавливали то или иное ПО.

Кроме того, наши специалисты обнаружили несколько новых представителей семейства троянов Android.Joker. Их основные функции — загрузка и выполнение произвольного кода, перехват содержимого поступающих уведомлений и подписка на платные сервисы без согласия владельцев Android-устройств.

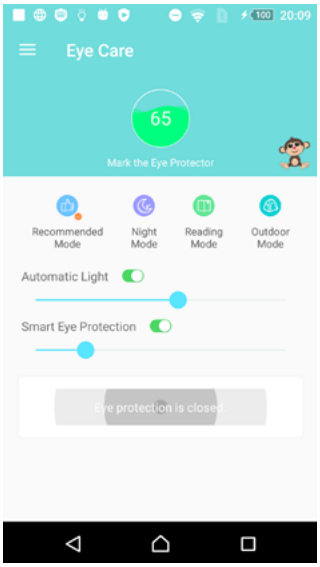
ГЛАВНЫЕ ТЕНДЕНЦИИ НОЯБРЯ

- Снижение общего числа угроз, обнаруженных на Android-устройствах
- Появление новых вредоносных приложений в каталоге Google Play

«Доктор Веб»: обзор вирусной активности для мобильных устройств в ноябре 2020 года

Угроза месяца

В середине ноября вирусные аналитики компании «Доктор Веб» выявили в Google Play трояна Android.Mixi.44.origin, который был встроен в приложение для заботы о зрении пользователей Android-устройств. Оно действительно выполняло заявленную функцию, но также имело и скрытые возможности.



Так, Android.Mixi.44.origin загружал веб-сайты и демонстрировал их поверх окон других приложений и интерфейса операционной системы, мешая нормальной работе с устройством. Содержимое этих сайтов могло быть любым: от рекламных баннеров и видеороликов до фишинговых страниц.

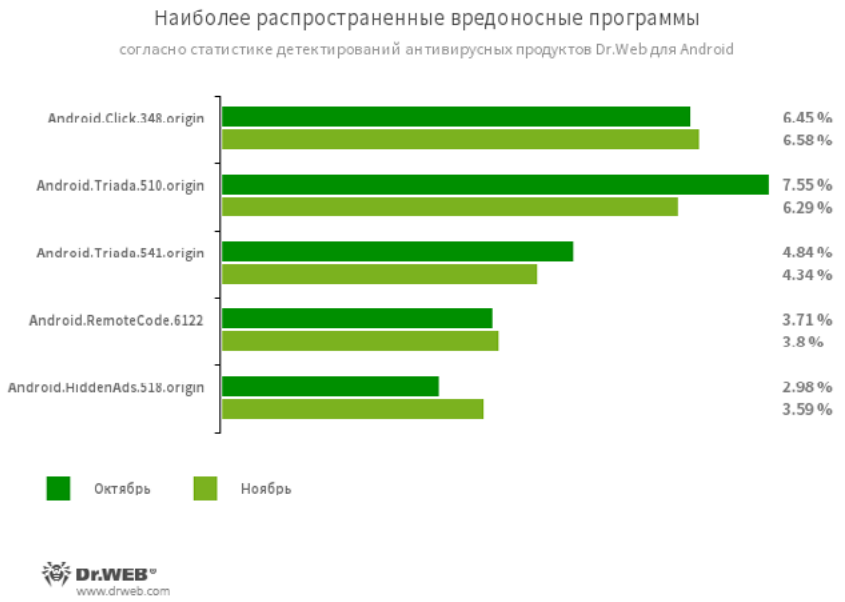
Другой функцией трояна был незаметный переход по ссылкам. Android.Mixi.44.origin получал от злоумышленников список веб-адресов, которые ему необходимо было посетить. Таким образом вредоносная программа искусственно увеличивала популярность сайтов, за что ее авторы получали вознаграждение.

Кроме того, троян пытался заработать на недавно выполненных установках программ. Для этого он отслеживал, какие приложения устанавливает и удаляет пользователь. Если получаемые в командах ссылки вели на страницы приложений в Google Play, Android.Mixi.44.origin проверял, были ли эти приложения уже установлены ранее. Если да, троян передавал в сервис аналитики информацию об именах пакетов этих программ вместе с реферал-идентификатором злоумышленников. Тем самым он пытался присвоить установки мошенникам, к которым те не имели никакого отношения. Если же такие программы еще не устанавливались, троян запоминал их и ожидал момента, когда пользователь их установит, после чего аналогичным образом пытался обмануть сервис.

Подробнее об Android.Mixi.44.origin рассказано в соответствующем новостном материале на сайте компании «Доктор Веб».

«Доктор Веб»: обзор вирусной активности для мобильных устройств в ноябре 2020 года

По данным антивирусных продуктов Dr.Web для Android



Android.Click.348.origin
Вредоносное приложение, которое самостоятельно загружает веб-сайты, нажимает на рекламные баннеры и переходит по ссылкам. Может распространяться под видом безобидных программ, не вызывая подозрений у пользователей.
Android.Triada.510.origin
Android.Triada.541.origin
Многофункциональные трояны, выполняющие разнообразные вредоносные действия. Относятся к семейству троянских приложений, проникающих в процессы всех работающих программ. Различные представители этого семейства могут встречаться в прошивках Android-устройств, куда злоумышленники внедряют их на этапе производства. Кроме того, некоторые их модификации могут эксплуатировать уязвимости, чтобы получить доступ к защищенным системным файлам и директориям.
Android.RemoteCode.6122
Вредоносная программа, которая загружает и выполняет произвольный код. В зависимости от модификации она также может загружать различные веб-сайты, переходить по ссылкам, нажимать на рекламные баннеры, подписывать пользователей на платные услуги и выполнять другие действия.
Android.HiddenAds.518.origin
Троян, предназначенный для показа навязчивой рекламы. Распространяется под видом популярных приложений другими вредоносными программами, которые в некоторых случаях незаметно устанавливают его в системный каталог.

«Доктор Веб»: обзор вирусной активности для мобильных устройств в ноябре 2020 года

По данным антивирусных продуктов Dr.Web для Android

Program.FreeAndroidSpy.1.origin

Program.Reptilicus.7.origin

Program.Mrecorder.1.origin

Приложения, которые следят за владельцами Android-устройств и могут использоваться для кибершпионажа. Они способны контролировать местоположение устройств, собирать данные об СМС-переписке, беседах в социальных сетях, копировать документы, фотографии и видео, прослушивать телефонные звонки и окружение и т. п.

Program.FakeAntiVirus.2.origin

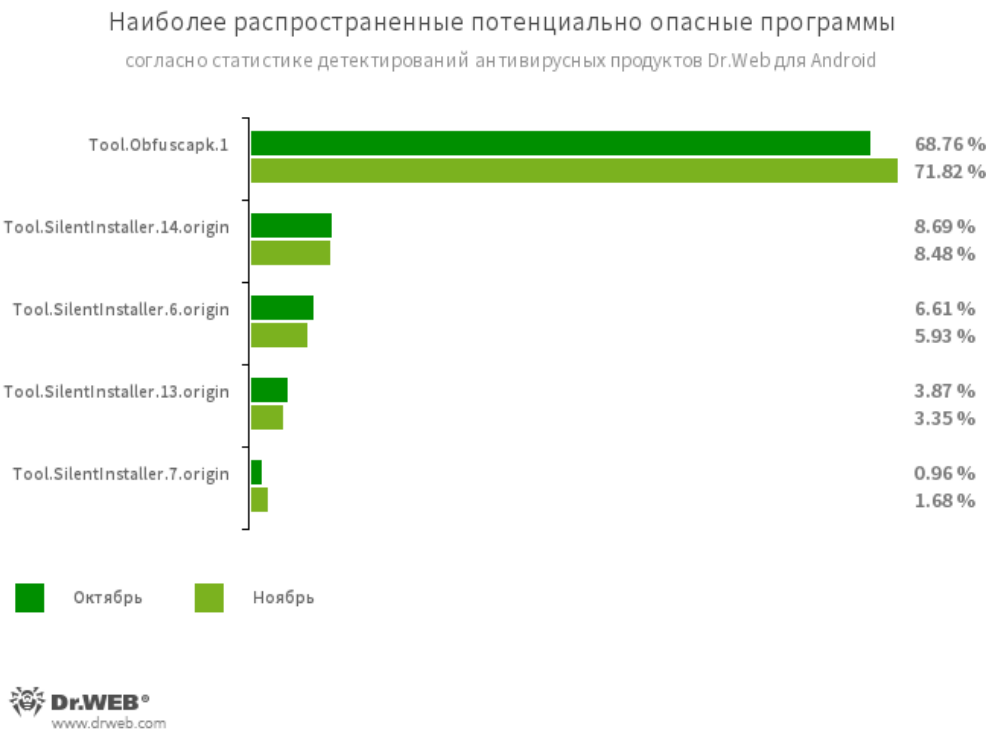
Детектирование рекламных программ, которые имитируют работу антивирусного ПО. Такие программы могут сообщать о несуществующих угрозах и вводить пользователей в заблуждение, требуя оплатить покупку полной версии.

Program.CreditSpy.2

Детектирование программ, предназначенных для присвоения кредитного рейтинга на основании персональных данных пользователей. Такие приложения загружают на удаленный сервер СМС-сообщения, информацию о контактах из телефонной книги, историю вызовов, а также другие сведения.

«Доктор Веб»: обзор вирусной активности для мобильных устройств в ноябре 2020 года

По данным антивирусных продуктов Dr.Web для Android



Tool.Obfuscapk.1

Детектирование приложений, защищенных утилитой-обфускатором Obfuscapk. Эта утилита используется для автоматической модификации и запутывания исходного кода Android-приложений, чтобы усложнить их обратный инжиниринг. Злоумышленники применяют ее для защиты вредоносных и других опасных программ от обнаружения антивирусами.

Tool.SilentInstaller.14.origin

Tool.SilentInstaller.6.origin

Tool.SilentInstaller.13.origin

Tool.SilentInstaller.7.origin

Потенциально опасные программные платформы, которые позволяют приложениям запускать apk-файлы без их установки. Они создают виртуальную среду исполнения, которая не затрагивает основную операционную систему.

«Доктор Веб»: обзор вирусной активности для мобильных устройств в ноябре 2020 года

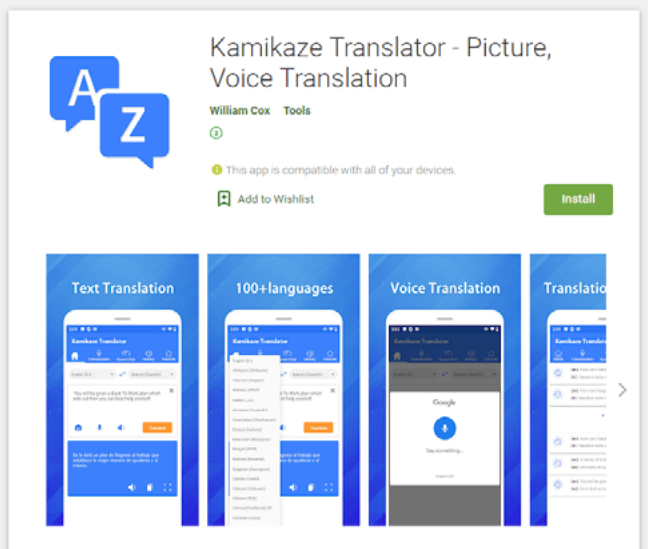
По данным антивирусных продуктов Dr.Web для Android

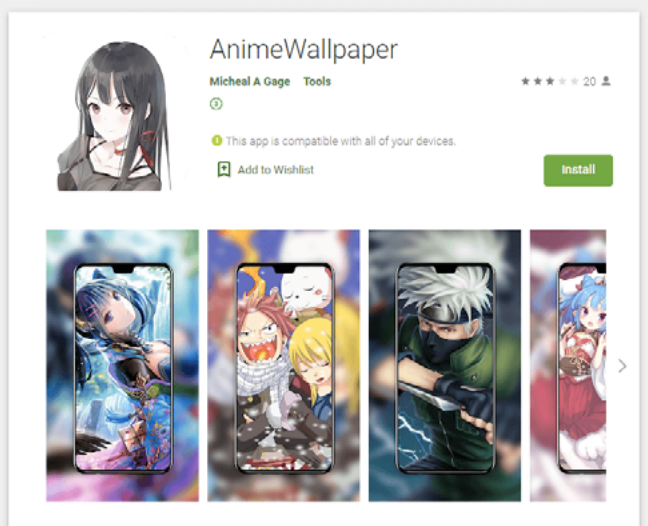
Программные модули, встраиваемые в Android-приложения и предназначенные для показа навязчивой рекламы на мобильных устройствах. В зависимости от семейства и модификации они могут демонстрировать рекламу в полноэкранном режиме, блокируя окна других приложений, выводить различные уведомления, создавать ярлыки и загружать веб-сайты.

- Adware.Adpush.36.origin
- Adware.SspSdk.1.origin
- Adware.Adpush.6547
- Adware.Myteam.2.origin
- Adware.Toofan.1.origin

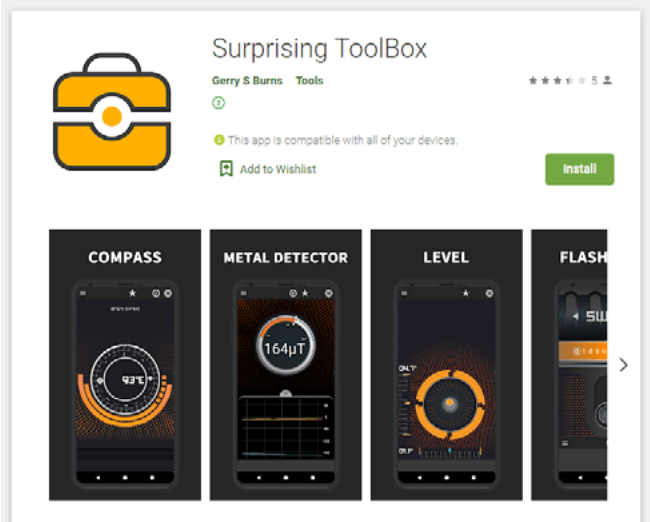
Угрозы в Google Play

Наряду с Android.Mixi.44.origin в течение последнего осеннего месяца вирусные аналитики компании «Доктор Веб» обнаружили в каталоге Google Play несколько новых модификаций троянов семейства Android.Joker. Они были добавлены в вирусную базу Dr.Web как Android.Joker.418, Android.Joker.419 и Android.Joker.452. Эти трояны распространялись под видом безобидных приложений — программы-переводчика, сборника изображений, а также утилиты с большим набором функций, таких как компас, фонарик, уровень и др.





Угрозы в Google Play



Вредоносные приложения загружали и выполняли произвольный код, а также могли подписывать пользователей на платные мобильные сервисы, перехватывая из поступающих уведомлений коды подтверждения для подключаемых услуг.

Для защиты Android-устройств от вредоносных и нежелательных программ пользователям следует установить антивирусные продукты Dr.Web для Android.

«Доктор Веб»: обзор вирусной активности для мобильных устройств в ноябре 2020 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