Dr.WEB®
с 1992 года

«Доктор Веб»: обзор вирусной активности для мобильных устройств в апреле 2019 года

Обзор вирусной активности для мобильных устройств в апреле 2019 года

30 апреля 2019 года

В апреле компания «Доктор Веб» сообщила о троянце Android.InfectionAds.1, который эксплуатировал несколько критических уязвимостей ОС Android. Они позволяли ему заражать другие программы, а также удалять и устанавливать ПО без участия пользователя. Кроме того, вирусные аналитики выявили новые модификации банковского троянца Android.Banker.180.origin, предназначенные для кражи денег у клиентов японских кредитных организаций. Были обнаружены очередные вредоносные приложения, которые распространялись через каталог Google Play. Среди них — троянцы-загрузчики Android.DownLoader, скачивавшие Android-банкеров на мобильные устройства, кликеры семейства Android.Click и стилеры Android.PWS.Instagram, похищавшие логины и пароли пользователей Instagram. Также в вирусную базу Dr.Web были добавлены записи для детектирования других вредоносных программ.

Главные тенденции апреля

- Появление новых вредоносных приложений в каталоге Google Play
- Распространение банковских троянцев

Обзор вирусной активности для мобильных устройств в апреле 2019 года

Мобильная угроза месяца

В начале апреля компания «Доктор Веб» рассказала об опасном троянце Android.InfectionAds.1, которого злоумышленники встраивают в изначально безобидные программы и распространяют через сторонние каталоги Android-приложений. Этот троянец эксплуатирует критические уязвимостей ОС Android, с использованием которых заражает apk-файлы (уязвимость CVE-2017-13156), а также самостоятельно устанавливает и удаляет программы (уязвимость CVE-2017-13315). Кроме того, Android.InfectionAds.1 показывает надоедливые рекламные баннеры, мешающие нормальной работе с зараженными устройствами. Подробная информация об этом троянце доступна в нашей вирусной библиотеке.

Обзор вирусной активности для мобильных устройств в апреле 2019 года

По данным антивирусных продуктов Dr.Web для Android

Android.Backdoor.682.origin

Троянец, который выполняет команды злоумышленников и позволяет им контролировать зараженные мобильные устройства.

Android.HiddenAds.1102

Android.HiddenAds.261.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.RemoteCode.4411

Вредоносное приложение, предназначенное для загрузки и выполнения произвольного кода.

Android.DownLoader.812.origin

Троянец, загружающий другие вредоносные приложения.

Обзор вирусной активности для мобильных устройств в апреле 2019 года

По данным антивирусных продуктов Dr.Web для Android

Adware.Zeus.1

Adware.AdPush.33.origin

Adware.Toofan.1.origin

Adware.Jiubang.2

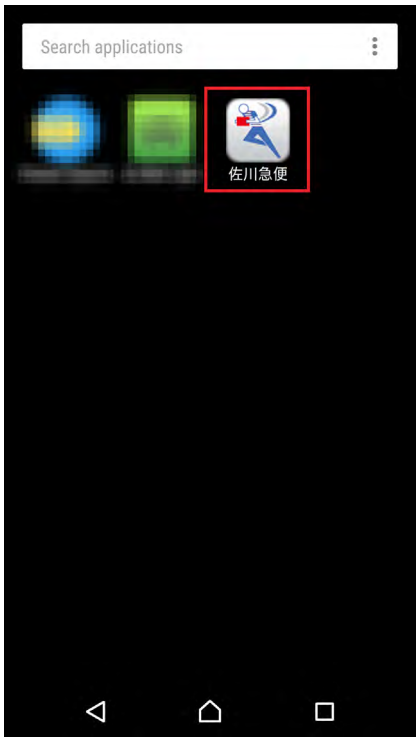
Нежелательные программные модули, встраиваемые в Android-приложения и предназначенные для показа навязчивой рекламы на мобильных устройствах.

Tool.VirtualApk.1.origin

Потенциально опасная программная платформа, которая позволяет приложениям запускать apk-файлы без их установки.

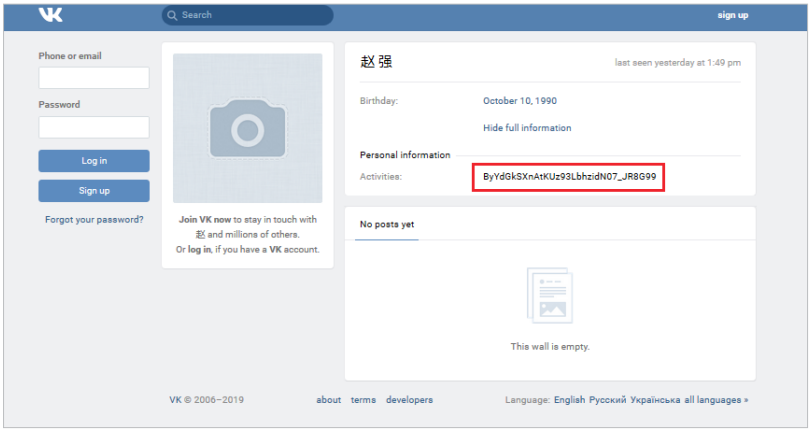
Android-банкеры

В уходящем месяце пользователям Android-устройств вновь угрожали банковские троянцы. В конце апреля вирусные аналитики «Доктор Веб» обнаружили новые модификации вредоносной программы Android.Banker.180.origin. Они распространялись под видом ПО для отслеживания посылок (например, приложения под названием «佐川急便») и предназначались для японских пользователей. После запуска троянцы удаляют свой значок и скрываются от пользователя.



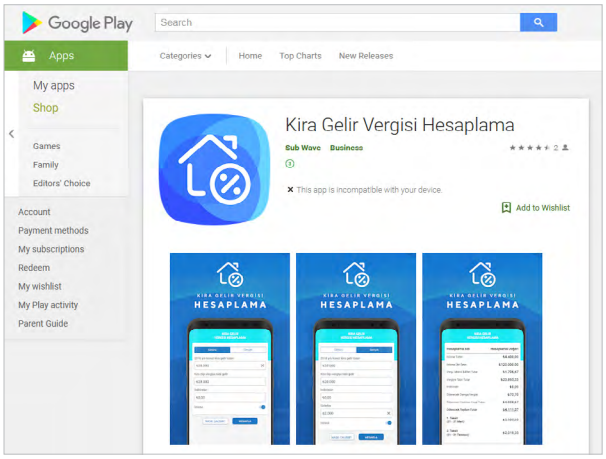
Эти модификации Android.Banker.180.origin контролируются через специально созданные страницы в социальной сети «ВКонтакте». На таких страницах в поле «Деятельность» («Activities») в зашифрованном виде располагается адрес одного из управляющих серверов банкера. Вредоносная программа ищет это поле с помощью регулярного выражения, расшифровывает адрес и подключается к серверу.

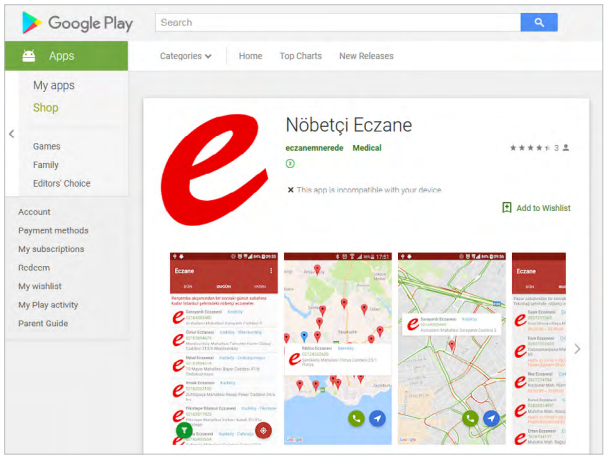
Угрозы в Google Play



Эти версии троянца перехватывают и отправляют СМС-сообщения по команде злоумышленников, показывают фишинговые окна, способны выполнять телефонные звонки и прослушивать окружение с использованием микрофона зараженного устройства. Помимо этого, они могут управлять смартфонами и планшетами: самостоятельно включать Wi-Fi-модуль, устанавливать интернет-соединение через мобильную сеть, блокировать экран и т. д.

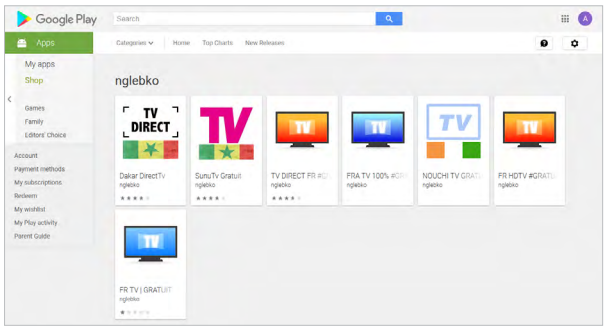
Кроме того, различных Android-банкеров скачивали на мобильные устройства обнаруженные в Google Play очередные загрузчики семейства Android.DownLoader, такие как Android.DownLoader.**4303**. Они распространялись под видом финансовых приложений.

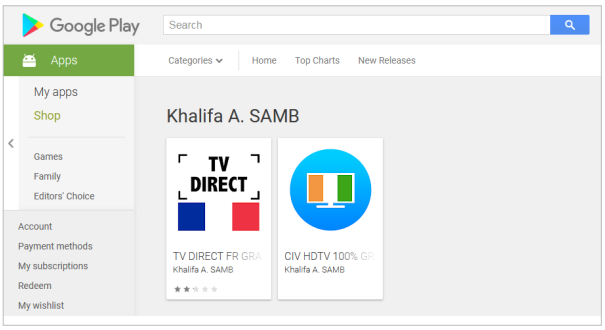


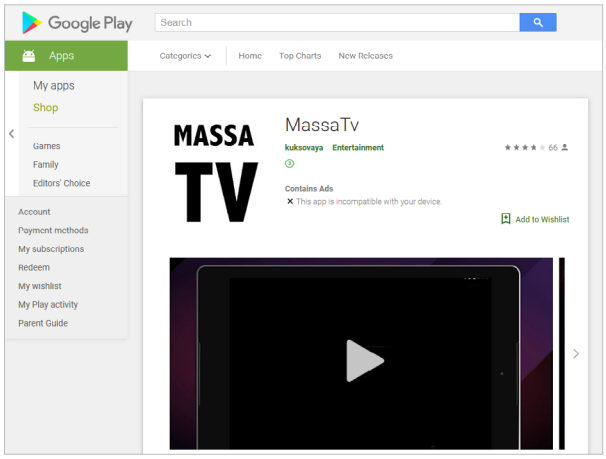


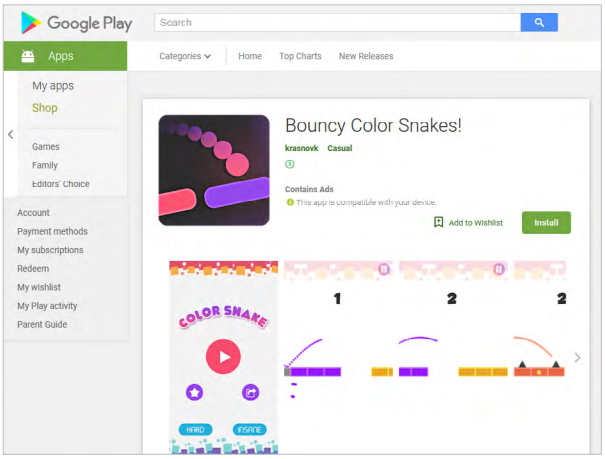
Троянцы в Google Play

Помимо загрузчиков в каталоге Google Play были выявлены и другие троянцы, такие как Android.Click.303.origin и Android.Click.304.origin. Они распространялись под видом безобидных приложений — игр и программ для просмотра телевизионных каналов. Вирусные аналитики «Доктор Веб» обнаружили 36 таких троянцев. Их загрузили свыше 151 000 пользователей.







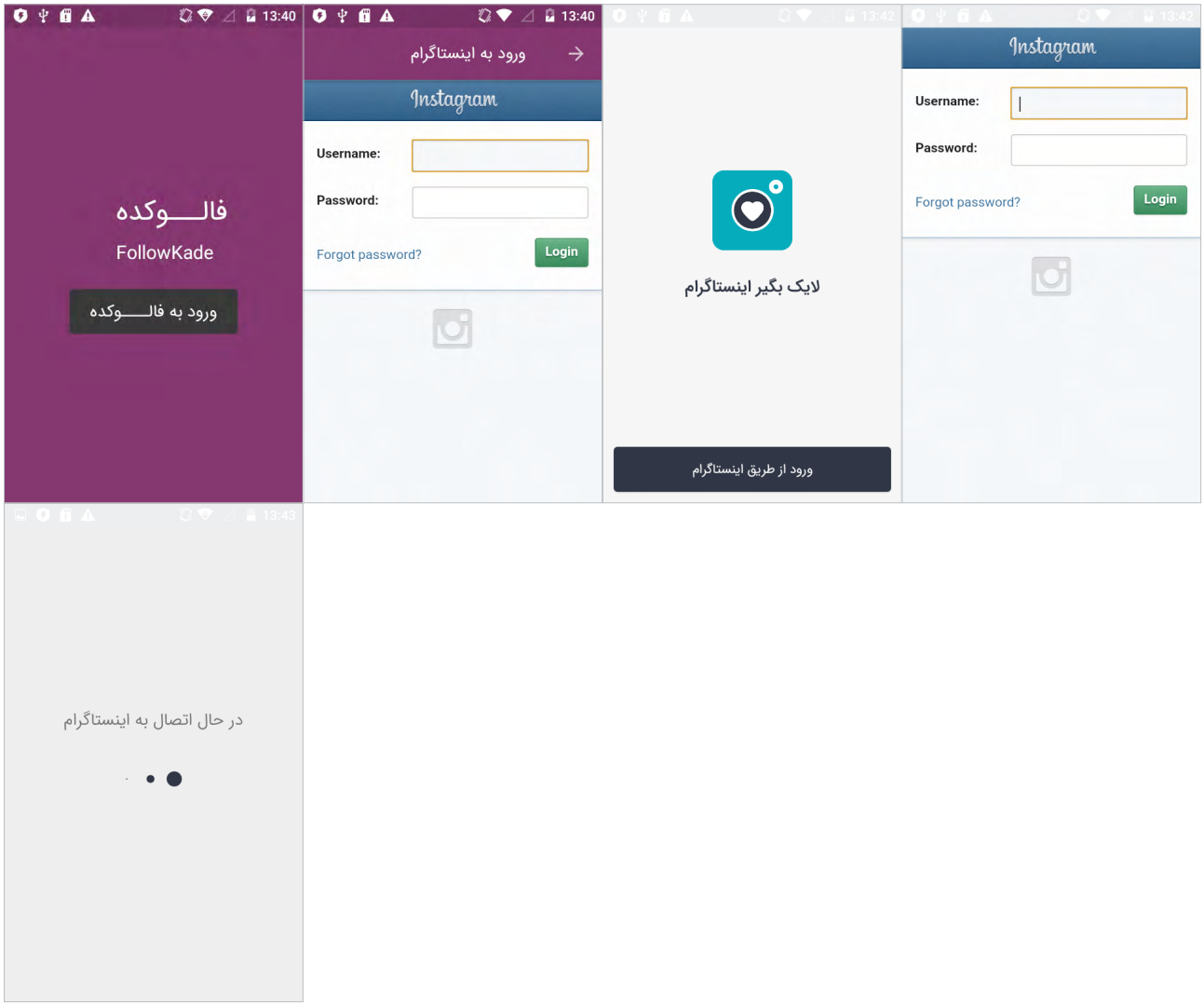


Эти вредоносные программы открывают невидимую активность с несколькими элементами WebView, в одном из которых загружают веб-сайт для получения от него управляющих команд. В других WebView они могут загружать различные скрипты JavaScript и заданные злоумышленниками сайты, на которых симулируют действия пользователей. Там они переходят по ссылкам и рекламным баннерам, накручивая счетчики посещений и кликов. Кроме того, нажатием на специально сформированные кнопки на этих сайтах они могут подписывать владельцев мобильных устройств на платные услуги, если мобильные операторы жертв поддерживают технологию быстрых подписок Wap-Click. Для затруднения удаления троянцы скрывают свои значки из меню главного экрана операционной системы.

Обзор вирусной активности для мобильных устройств в апреле 2019 года

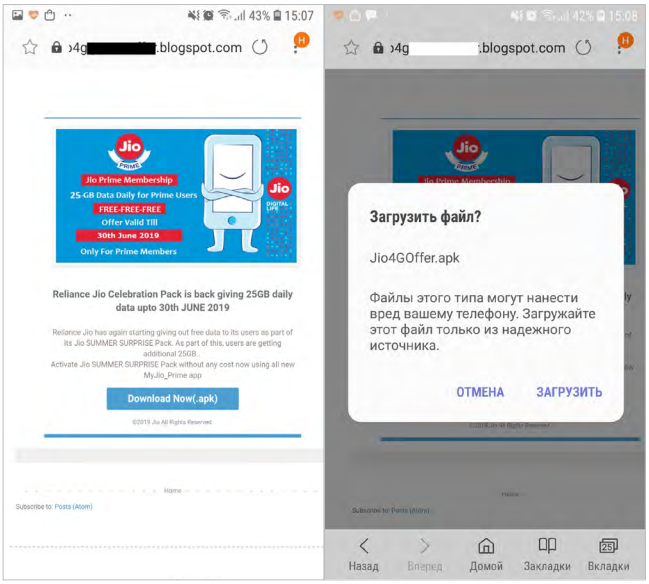
Троянцы в Google Play

В конце месяца в вирусную базу Dr.Web были добавлены записи для детектирования троянцев Android.PWS.Instagram.4 и Android.PWS.Instagram.5. Киберпреступники распространяли их под видом полезных программ для пользователей Instagram — для накрутки «лайков» и числа подписчиков, а также для повышения безопасности учетной записи. При запуске троянцы запрашивали у потенциальных жертв их логин и пароль, которые затем передавались на сервер злоумышленников.



Другие угрозы

Среди прочих вредоносных приложений, угрожавших владельцам Android-смартфонов и планшетов в апреле, был троянец Android.FakeApp.2.origin. Он скрывался в программе, якобы предоставлявшей 25 ГБ бесплатного интернет-трафика абонентам индийского мобильного оператора Jio.



Для распространения среди большего числа пользователей троянец отправлял СМС-сообщения со ссылкой на страницу загрузки своей копии на номера абонентов из телефонной книги зараженного устройства. Основное предназначение Android.FakeApp.2.origin — показ рекламных баннеров.

Среди угрожающих владельцам Android-устройств троянцев встречаются самые разные вредоносные приложения, которые распространяются через веб-сайты и официальный каталог Google Play. Для защиты смартфонов и планшетов следует установить антивирусные продукты Dr.Web для Android.

Обзор вирусной активности для мобильных устройств в апреле 2019 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