

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



Обзор вирусной активности для мобильных устройств в ноябре 2018 года

30 ноября 2018 года

В последнем осеннем месяце этого года вирусные аналитики «Доктор Веб» выявили нового банковского троянца для ОС Android. Он распространялся через каталог Google Play и атаковал клиентов европейских кредитных организаций. Кроме того, в течение ноября в Google Play были обнаружены другие троянцы, а также нежелательные программы.

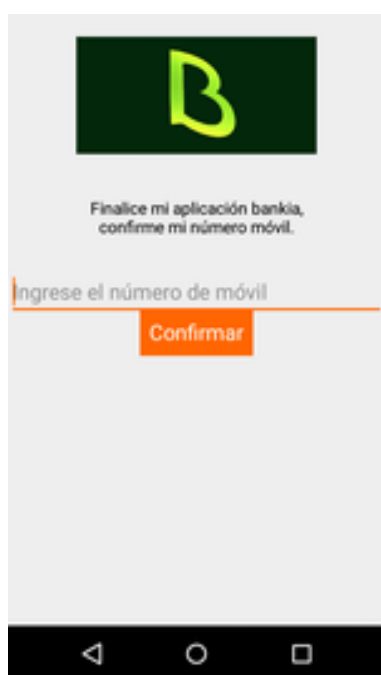
Главные тенденции ноября

- Распространение вредоносных и нежелательных программ в каталоге Google Play

Обзор вирусной активности для мобильных устройств в ноябре 2018 года

Мобильная угроза месяца

В середине ноября специалисты компании «Доктор Веб» выявили банковского троянца [Android.Banker.2876](#), который угрожал клиентам нескольких европейских кредитных организаций. Он крад конфиденциальную информацию, а также перехватывал и отправлял СМС-сообщения.



Особенности [Android.Banker.2876](#):

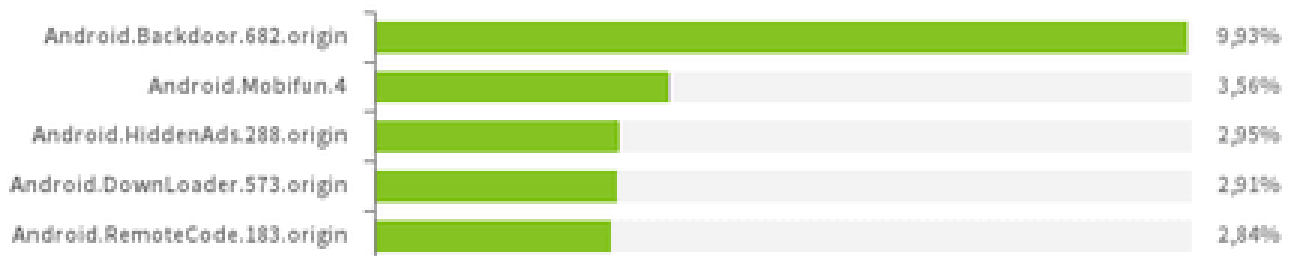
- распространялся через каталог Google Play;
- имитировал банковские приложения испанских, французских и немецких кредитных организаций;
- скрывал свой значок из списка приложений главного экрана;
- содержал встроенную игру, которую запускал после закрытия своего окна пользователем.

Подробнее об этом троянце рассказано в соответствующей новостной [публикации](#) на нашем сайте.

Обзор вирусной активности для мобильных устройств в ноябре 2018 года

По данным антивирусных продуктов Dr.Web для Android

Наиболее распространенные вредоносные программы согласно статистике детектирования антивирусных продуктов Dr.Web для Android



[Android.Backdoor.682.origin](#)

Троянская программа, которая выполняет команды злоумышленников и позволяет им контролировать зараженные мобильные устройства.

[Android.Mobifun.4](#)

Троянец, который загружает различные приложения.

[Android.HiddenAds.288.origin](#)

Троянец, предназначенный для показа навязчивой рекламы. Распространяется под видом популярных приложений другими вредоносными программами, которые в некоторых случаях незаметно устанавливают его в системный каталог.

[Android.DownLoader.573.origin](#)

Троянец, загружающий другие вредоносные приложения.

[Android.RemoteCode.183.origin](#)

Вредоносная программа, предназначенная для загрузки и выполнения произвольного кода.

Обзор вирусной активности для мобильных устройств в ноябре 2018 года

По данным антивирусных продуктов Dr.Web для Android

Наиболее распространенные
нежелательные и потенциально опасные программы
согласно статистике детектированных антивирусных продуктов Dr.Web для Android



Adware.Zeus.1

[Adware.Adpush.2514](#)

Adware.Patacore.1.origin

Adware.Avazu.5.origin

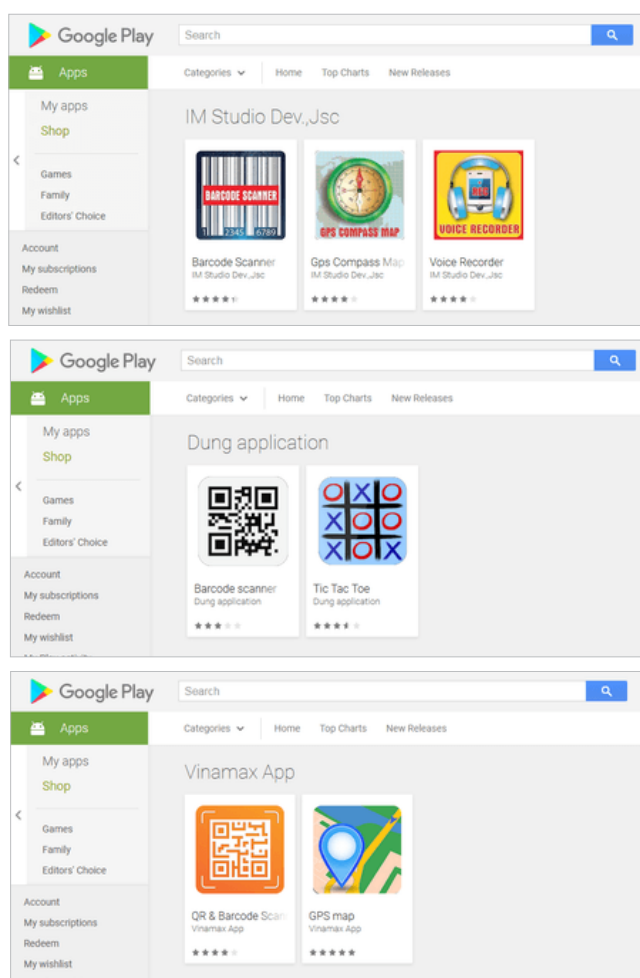
Adware.Gexin.2.origin

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

Обзор вирусной активности для мобильных устройств в ноябре 2018 года

Угрозы в Google Play

В начале ноября вирусные аналитики «Доктор Веб» обнаружили в каталоге Google Play приложения со встроенными в них нежелательными рекламными модулями [Adware.HiddenAds.7.origin](#) и [Adware.HiddenAds.8.origin](#). Они показывали рекламу даже тогда, когда содержащие их программы не использовались.



Позднее специалисты «Доктор Веб» выявили в Google Play очередных троянцев семейства [Android.FakeApp](#), добавленных в вирусную базу Dr.Web как [Android.FakeApp.138](#), [Android.FakeApp.139](#) и [Android.FakeApp.144](#). Они скрывались в приложениях, которые якобы позволяли получать деньги за участие в опросах. При запуске вредоносные программы загружали мошеннические веб-сайты, где потенциальной жертве предлагалось ответить на несколько вопросов. После этого для получения обещанного «вознаграждения» от пользователя требовалось оплатить некую комиссию за перевод средств, конвер-

Узнайте больше

[Лаборатория-live](#) | [Вирусные обзоры](#) | [Горячая лента угроз](#) | [Вирусная библиотека](#)

Обзор вирусной активности для мобильных устройств в ноябре 2018 года

Угрозы в Google Play

тацию валюты или за иную придуманную злоумышленниками процедуру. Если владелец зараженного устройства соглашался на оплату, запрашиваемая сумма оседала в карманах сетевых жуликов, а жертва мошенничества не получала ничего.



Кроме того, под видом различных утилит злоумышленники распространяли троянца-загрузчика [Android.DownLoader.832.origin](#). Он скачивал другие вредоносные приложения и пытался установить их.

Каталог Google Play остается одним из самых безопасных источников приложений для смартфонов и планшетов под управлением ОС Android, однако киберпреступникам по-прежнему удается распространять через него вредоносные программы. Для защиты мобильных устройств пользователям следует установить антивирусные продукты Dr.Web для Android.

Узнайте больше

[Лаборатория-live](#) | [Вирусные обзоры](#) | [Горячая лента угроз](#) | [Вирусная библиотека](#)

Обзор вирусной активности для мобильных устройств в ноябре 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

[ВебиОметр](#) | [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](#)



© ООО «Доктор Веб»,
2003-2018

Узнайте больше

[Лаборатория-live](#) | [Вирусные обзоры](#) | [Горячая лента угроз](#) | [Вирусная библиотека](#)