



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



Обзор вирусной активности для мобильных устройств в декабре 2018 года

28 декабря 2018 года

В начале декабря бразильских пользователей Android-устройств атаковал банковский троянец, распространявшийся через Google Play. Кроме того, в течение месяца в этом официальном каталоге ПО для Android были выявлены другие вредоносные приложения. В конце декабря специалисты «Доктор Веб» обнаружили новую версию коммерческой шпионской программы, собирающей большой объем конфиденциальной информации.

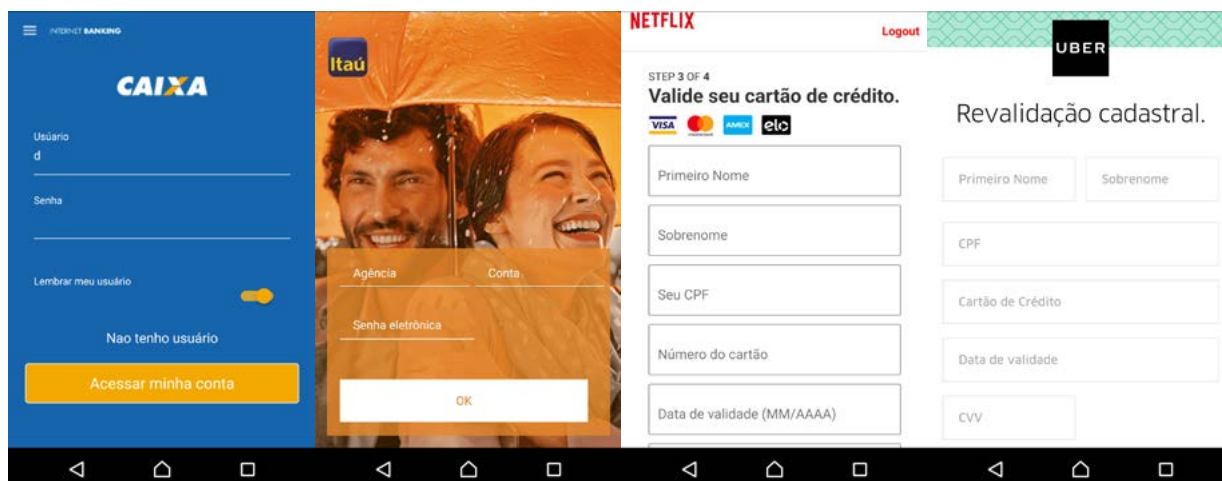
Главные тенденции декабря

- Распространение опасного банковского троянца, предназначенного для пользователей из Бразилии
- Обнаружение новой версии потенциально опасной программы, созданной для слежки за пользователями мобильных устройств
- Выявление множества вредоносных и нежелательных приложений в Google Play

Обзор вирусной активности для мобильных устройств в декабре 2018 года

Мобильная угроза месяца

В начале декабря вирусные аналитики исследовали банковского троянца [Android.BankBot.495.origin](#), атаковавшего клиентов бразильских кредитных учреждений. Эта вредоносная программа пыталась получить доступ к специальным возможностям (Accessibility Service) ОС Android, с использованием которых она самостоятельно управляла банковскими программами, считывала содержимое их окон и передавала злоумышленникам конфиденциальную информацию. Кроме того, [Android.BankBot.495.origin](#) показывал фишинговые окна поверх приложений и обманом получал от жертв пароли, логины, данные банковских карт и другие секретные сведения.

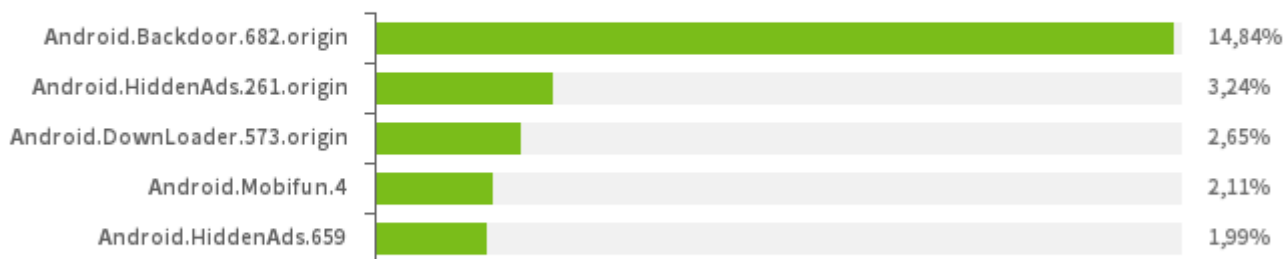


Подробнее об этом троянце рассказано в опубликованной на сайте компании «Доктор Веб» [НОВОСТИ](#).

Обзор вирусной активности для мобильных устройств в декабре 2018 года

По данным антивирусных продуктов Dr.Web для Android

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



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

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

[Android.HiddenAds.261.origin](#)

[Android.HiddenAds.659](#)

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.

[Android.Mobifun.4](#)

Троянец, который загружает различные приложения.

Обзор вирусной активности для мобильных устройств в декабре 2018 года

По данным антивирусных продуктов Dr.Web для Android

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



Adware.Zeus.1

[Adware.Patacore.1.origin](#)

[Adware.Adpush.2514](#)

Adware.AdPush.29.origin

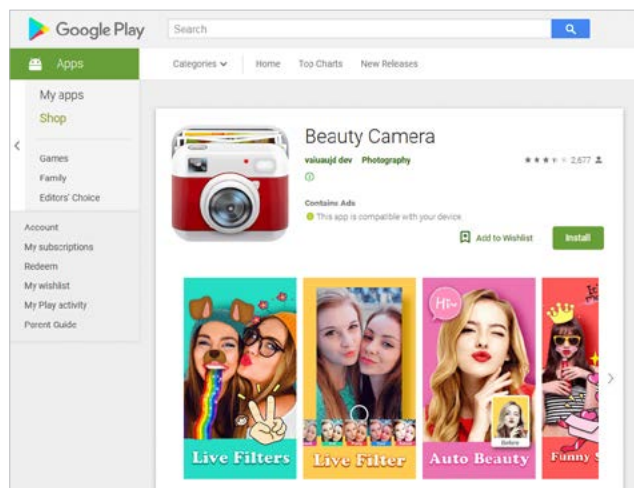
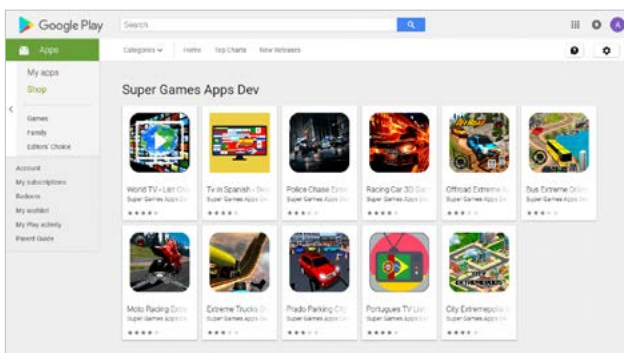
Adware.Jiubang.2

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

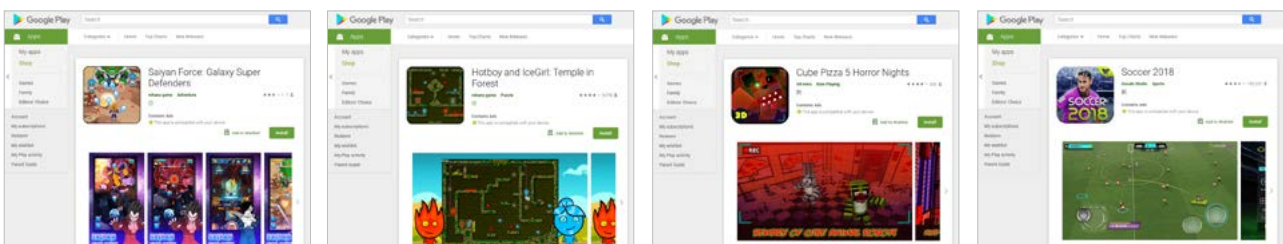
Обзор вирусной активности для мобильных устройств в декабре 2018 года

Угрозы в Google Play

В течение месяца в Google Play было выявлено множество вредоносных и нежелательных программ. Среди них — рекламные троянцы [Android.HiddenAds.343.origin](#) и [Android.HiddenAds.847](#), распространявшиеся под видом игр и полезных приложений. После запуска они скрывали свой значок с главного экрана и начинали показывать рекламу.



Также были выявлены программы со встроенными нежелательными модулями [Adware.Patacore](#) и [Adware.HiddenAds](#). Они демонстрировали рекламу даже тогда, когда содержащее их ПО не было запущено. В общей сложности такие программы установили свыше 5 300 000 пользователей.



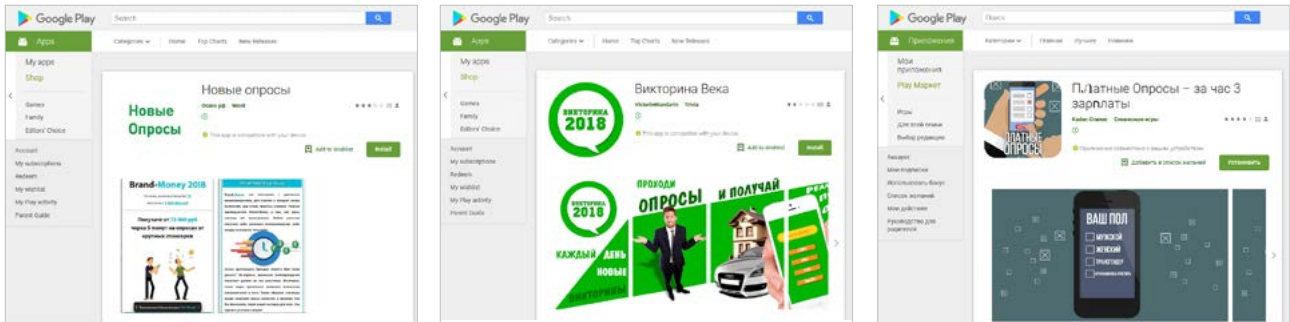
Злоумышленники вновь распространяли мошеннические приложения. В вирусную базу Dr.Web были добавлены записи для детектирования троянцев [Android.FakeApp.149](#), [Android.FakeApp.151](#) и [Android.FakeApp.152](#). Эти вредоносные программы загружали веб-страницы, на которых потенциальным жертвам предлагалось за вознаграждение ответить на вопросы. Для получения «оплаты» от пользователя требовалось выполнить проверочный платеж, однако после перевода средств киберпреступникам владельцы зараженных устройств не получали ничего.

Узнайте больше

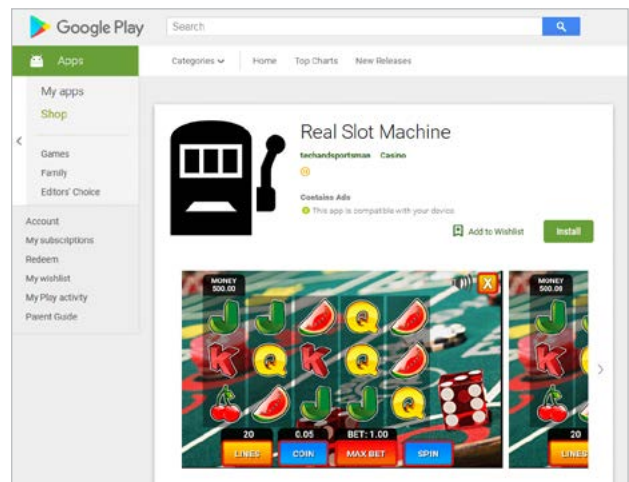
[Лаборатория-live](#) | [Вирусные обзоры](#) | [Горячая лента угроз](#) | [Вирусная библиотека](#)

Обзор вирусной активности для мобильных устройств в декабре 2018 года

Угрозы в Google Play



Кроме того, вирусные аналитики обнаружили троянца [Android.Proxy.4.origin](#), которого вирусописатели использовали для перенаправления трафика через смартфоны и планшеты их владельцев. [Android.Proxy.4.origin](#) скрывался в безобидных на первый взгляд играх.



Обзор вирусной активности для мобильных устройств в декабре 2018 года

Кибершпионаж

Среди выявленных в декабре потенциально опасных программ оказалась новая версия коммерческого шпиона [Program.Spyzie.1.origin](#), который позволяет следить за пользователями Android-устройств. Он перехватывает содержимое СМС и сообщений электронной почты, отслеживает телефонные звонки, историю посещений веб-браузера, координаты зараженного смартфона или планшета, получает доступ к переписке в популярных программах для онлайн-общения, а также крадет другую информацию.

Пользователям ОС Android угрожают различные вредоносные и нежелательные программы, которые распространяются как при помощи веб-сайтов, так и через каталог Google Play. Кроме того, злоумышленники могут устанавливать их самостоятельно, если получат физический доступ к мобильным устройствам. Для защиты смартфонов и планшетов их владельцам следует установить антивирусные продукты Dr.Web для Android.

Обзор вирусной активности для мобильных устройств в декабре 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](#)