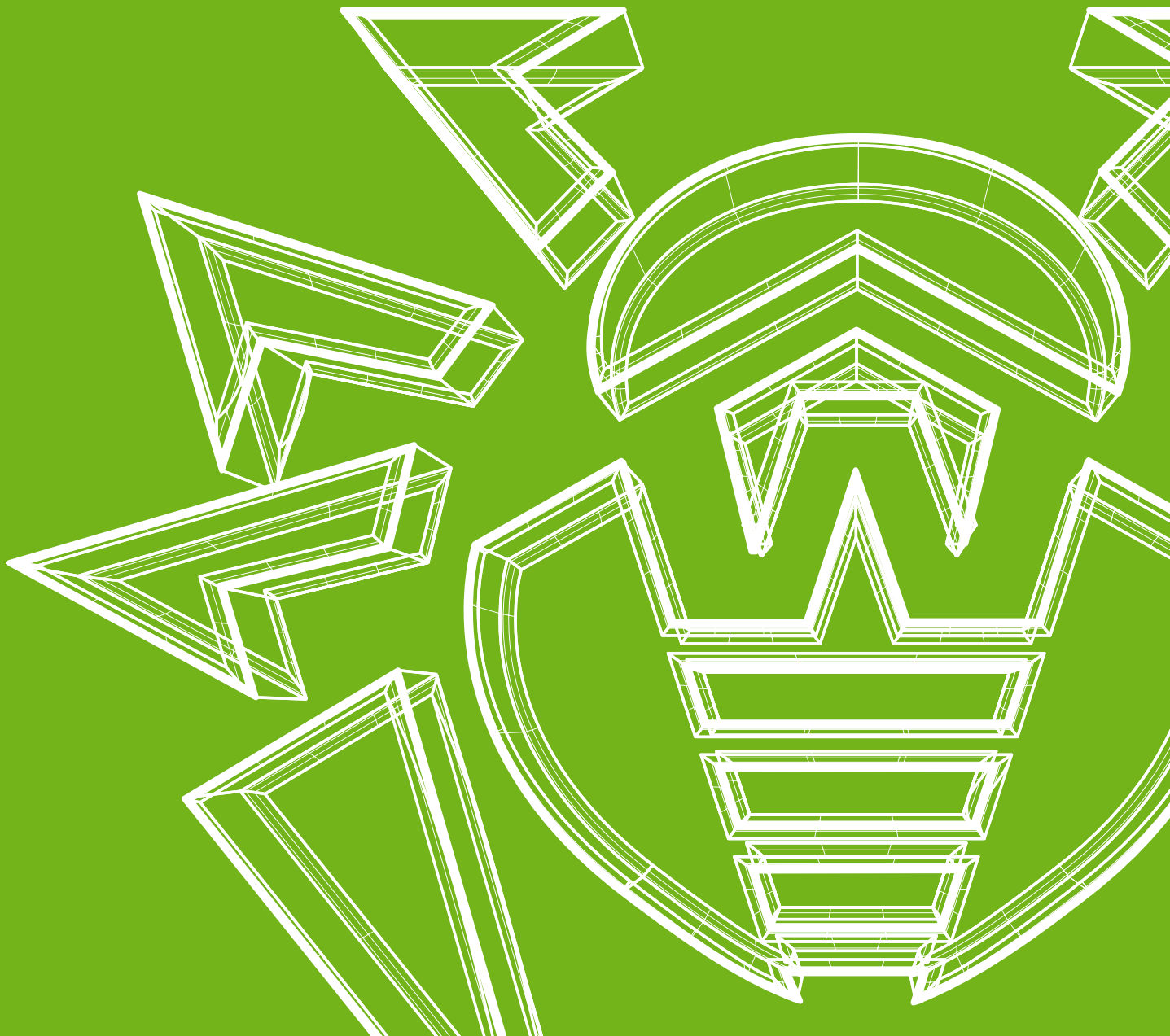
Dr.WEB®
с 1992 года

«Доктор Веб»: обзор вирусной активности для мобильных устройств в ноябре 2021 года



«Доктор Веб»: обзор вирусной активности для мобильных устройств в ноябре 2021 года

9 декабря 2021 года

Согласно статистике детектирований антивирусных продуктов Dr.Web для Android, в ноябре владельцы Android-устройств чаще всего сталкивались с рекламными троянами. Среди наиболее распространенных угроз остаются и различные вредоносные программы, способные загружать другие приложения и выполнять произвольный код.

В начале месяца компания «Доктор Веб» опубликовала исследование, направленное на оценку безопасности детских смарт-часов. Оно показало, что в подобных устройствах могут встречаться различные уязвимости, в том числе предустановленные троянские приложения.

В течение ноября наши специалисты обнаружили новые вредоносные программы в каталоге Google Play. Среди них — трояны семейств Android.PWS.Facebook и Android.Joker. Первые похищают данные, необходимые для взлома учетных записей Facebook. Вторые подписывают жертв на платные мобильные услуги. Очередная угроза была выявлена и в каталоге AppGallery. Злоумышленники распространяли в нем игры со встроенным трояном Android.Cynos.7.origin, который передавал на удаленный сервер информацию о мобильных номерах пользователей, а также их устройствах.

ГЛАВНЫЕ ТЕНДЕНЦИИ НОЯБРЯ

- Рекламные трояны остаются в числе наиболее распространенных угроз для пользователей Android-устройств
- Обнаружение новых троянов в каталоге Google Play
- Обнаружение очередной угрозы в каталоге AppGallery

Угроза месяца

В конце ноября компания «Доктор Веб» сообщила об обнаружении в каталоге AppGallery десятков различных игр, в которые был встроен троян Android.Cynos.7.origin. Он собирал и передавал злоумышленникам информацию о мобильных номерах пользователей и их устройствах. Кроме того, вредоносная программа демонстрировала рекламу. Подробнее об этой угрозе рассказано в нашем новостном материале.чных игр, в которые был встроен троян Android.Cynos.7.origin. Он собирал и передавал злоумышленникам информацию о мобильных номерах пользователей и их устройствах. Кроме того, вредоносная программа демонстрировала рекламу. Подробнее об этой угрозе рассказано в нашем новостном материале.

«Доктор Веб»: обзор вирусной активности для мобильных устройств в ноябре 2021 года

По данным антивирусных продуктов Dr.Web для Android

Android.HiddenAds.3018

Android.HiddenAds.1994

Android.HiddenAds.615.origin

Трояны, предназначенные для показа навязчивой рекламы. Представители этого семейства часто распространяются под видом безобидных приложений и в некоторых случаях устанавливаются в системный каталог другими вредоносными программами. Попадая на Android-устройства, такие рекламные трояны обычно скрывают от пользователя свое присутствие в системе — например, «прячут» значок приложения из меню главного экрана. Android.HiddenAds.3018 является новой версией трояна Android.HiddenAds.1994.

Android.Triada.4567

Многофункциональный троян, выполняющий разнообразные вредоносные действия. Относится 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.MobiDash.6244

Троянская программа, показывающая надоедливую рекламу. Представляет собой программный модуль, который разработчики ПО встраивают в приложения.

«Доктор Веб»: обзор вирусной активности для мобильных устройств в ноябре 2021 года

По данным антивирусных продуктов Dr.Web для Android

Program.FakeAntiVirus.1

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.SecretVideoRecorder.1.origin

Приложение, предназначенное для фоновой фото- и видеосъемки через встроенные камеры Android-устройств. Оно может работать незаметно, позволяя отключить уведомления о записи, а также изменять значок и описание приложения на фальшивые. Такая функциональность делает данную программу потенциально опасной.

Program.FreeAndroidSpy.1.origin

Program.Gemius.1.origin

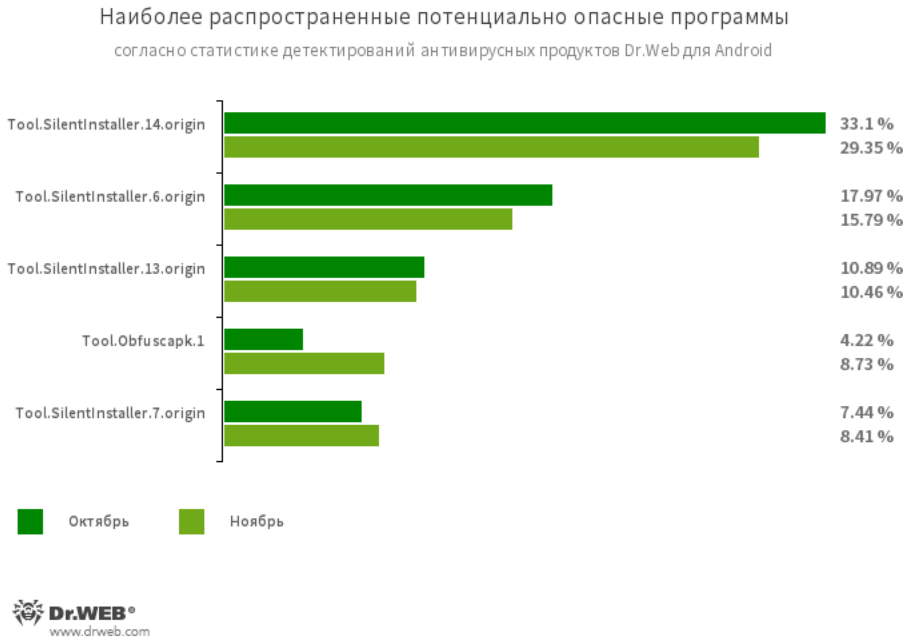
Приложения, которые следят за владельцами Android-устройств и могут использоваться для кибершпионажа. Они способны контролировать местоположение устройств, собирать данные об СМС-переписке, беседах в социальных сетях, копировать документы, фотографии и видео, прослушивать телефонные звонки и окружение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

Program.KeyStroke.3

Android-программа, способная перехватывать вводимую на клавиатуре информацию. Некоторые ее модификации также позволяют отслеживать входящие СМС-сообщения, контролировать историю телефонных звонков и выполнять запись телефонных разговоров.

«Доктор Веб»: обзор вирусной активности для мобильных устройств в ноябре 2021 года

По данным антивирусных продуктов Dr.Web для Android



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.

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.

«Доктор Веб»: обзор вирусной активности для мобильных устройств в ноябре 2021 года

По данным антивирусных продуктов Dr.Web для Android

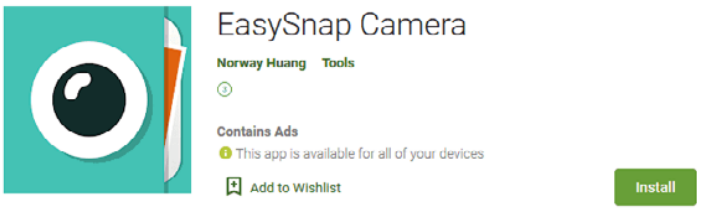
Программные модули, встраиваемые в Android-приложения и предназначенные для показа навязчивой рекламы на мобильных устройствах. В зависимости от семейства и модификации они могут демонстрировать рекламу в полноэкранном режиме, блокируя окна других приложений, выводить различные уведомления, создавать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

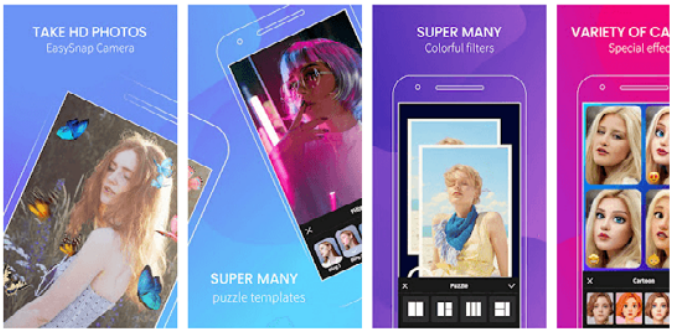
- Adware.SspSdk.1.origin
- Adware.AdPush.36.origin
- Adware.Adpush.16510
- Adware.Myteam.2.origin
- Adware.Fictus.1.origin

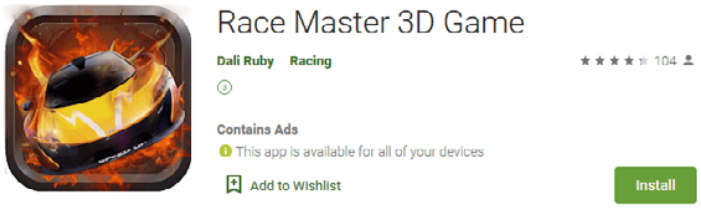
«Доктор Веб»: обзор вирусной активности для мобильных устройств в ноябре 2021 года

Угрозы в Google Play

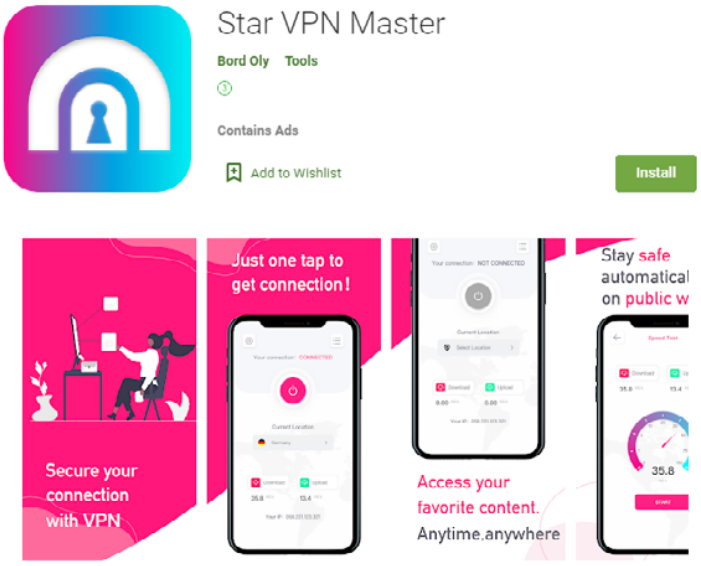
В минувшем месяце вирусные аналитики «Доктор Веб» выявили в каталоге Google Play новых троянов семейства Android.PWS.Facebook, предназначенных для кражи логинов, паролей и другой информации, необходимой для взлома учетных записей Facebook. Они были добавлены в вирусную базу Dr.Web как Android.PWS.Facebook.75, Android.PWS.Facebook.76, Android.PWS.Facebook.93 и Android.PWS.Facebook.97. Трояны распространялись под видом фоторедактора EasySnap Camera, гоночной игры Race Master 3D Game, а также VPN-клиентов Touch VPN Proxy и Star VPN Master.





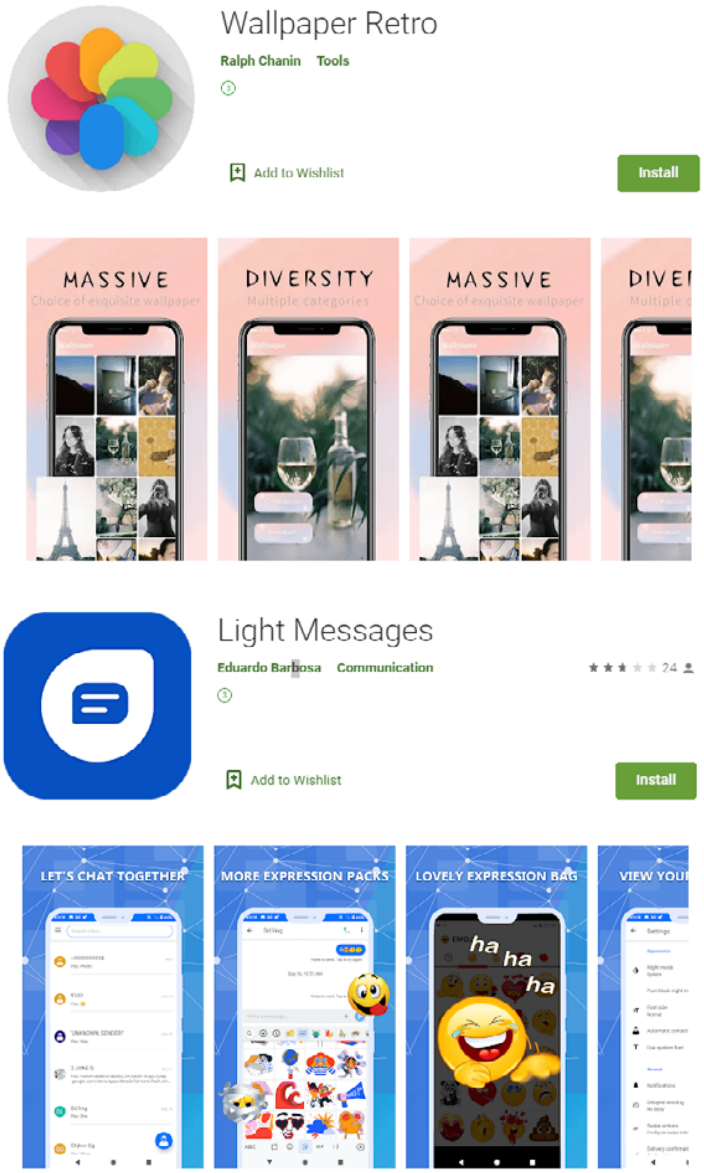


Угрозы в Google Play



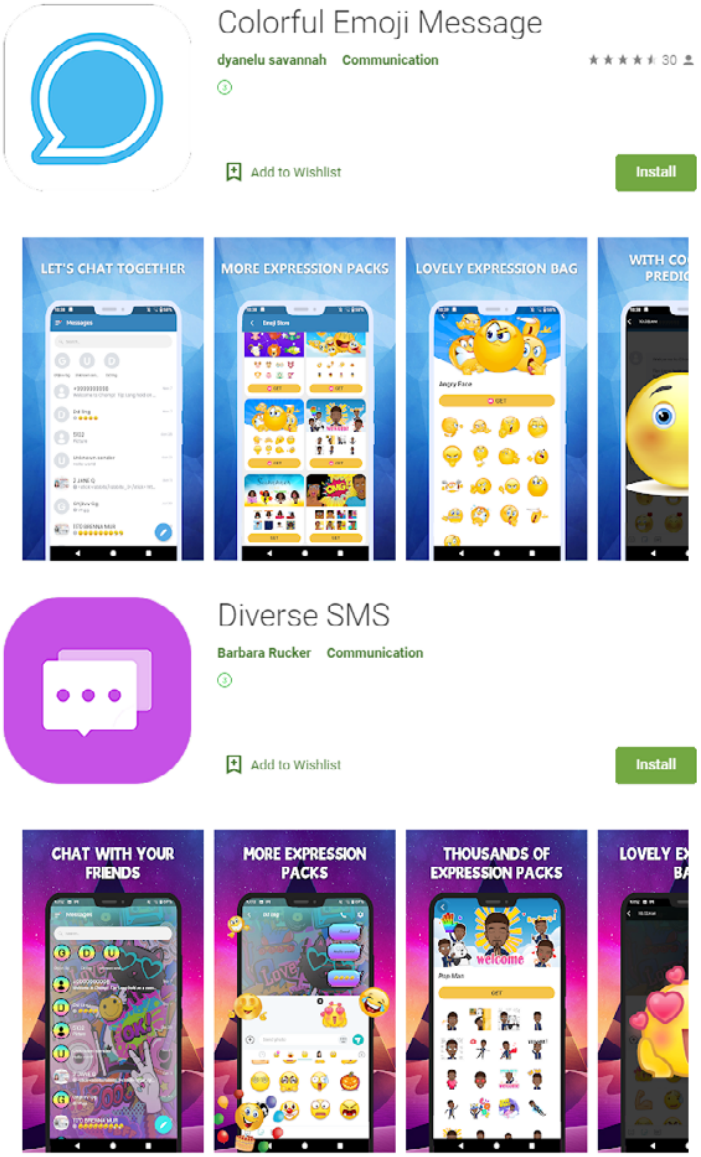
Кроме того, наши специалисты обнаружили очередных троянов семейства Android.Joker, получивших имена Android.Joker.1060, Android.Joker.1061, Android.Joker.1068 и Android.Joker.1076. Злоумышленники выдавали их за безобидные программы — сборник изображений Wallpaper Retro, а также мессенджеры Light Messages, Colorful Emoji Message и Diverse SMS. Попав на устройства пользователей, трояны подписывали тех на платные мобильные услуги и могли загружать и выполнять произвольный код.

Угрозы в Google Play



«Доктор Веб»: обзор вирусной активности для мобильных устройств в ноябре 2021 года

Угрозы в Google Play



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 2021 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
Центр противодействия кибер-мошенничеству

Пресс-центр
Официальная информация | Контакты для прессы | Брошюры | Галерея

Контакты
Центральный офис
125124 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

Узнайте больше
Лаборатория-live | Вирусные обзоры | Горячая лента угроз | Вирусная библиотека