Dr.WEB®
с 1992 года

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

Обзор вирусной активности для мобильных устройств в октябре 2019 года

13 ноября 2019 года

Второй осенний месяц этого года оказался неспокойным для владельцев Android-устройств. Вирусные аналитики «Доктор Веб» обнаружили в каталоге Google Play множество вредоносных программ – в частности, троянцев-кликеров Android.Click, которые подписывали пользователей на платные услуги. Среди найденных угроз также были вредоносные приложения семейства Android.Joker. Они тоже подписывали жертв на дорогостоящие сервисы и могли выполнять произвольный код. Кроме того, наши специалисты выявили других троянцев.

Главные тенденции октября

- Рост числа выявленных угроз в каталоге Google Play

Обзор вирусной активности для мобильных устройств в октябре 2019 года

Мобильная угроза месяца

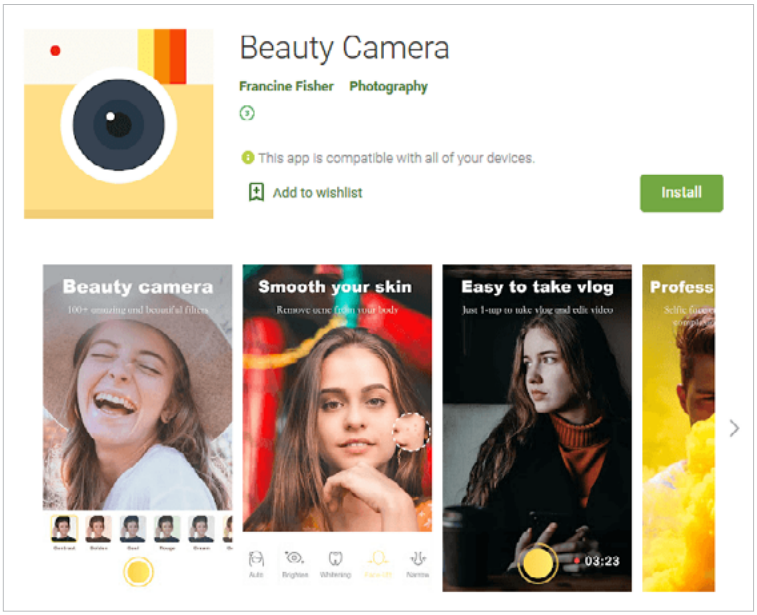
В начале октября компания «Доктор Веб» проинформировала пользователей о нескольких троянцах-кликерах, добавленных в вирусную базу Dr.Web как Android.Click.322.origin, Android.Click.323.origin и Android.Click.324.origin. Эти вредоносные приложения незаметно загружали веб-сайты, где самостоятельно подписывали своих жертв на платные мобильные сервисы. Особенности троянцев:

- встроены в безобидные программы;
- защищены коммерческим упаковщиком;
- маскируются под известные SDK;
- атакуют пользователей определенных стран.

В течение всего месяца наши вирусные аналитики выявляли и другие модификации этих кликеров — например, Android.Click.791, Android.Click.800, Android.Click.802, Android.Click.808, Android.Click.839, Android.Click.841. Позднее были найдены похожие на них вредоносные приложения, которые получили имена Android.Click.329.origin, Android.Click.328.origin и Android.Click.844. Они тоже подписывали жертв на платные услуги, но их разработчиками могли быть другие вирусописатели. Все эти троянцы скрывались в безобидных, на первый взгляд, программах — фотокамерах, фоторедакторах и сборниках обоев для рабочего стола.

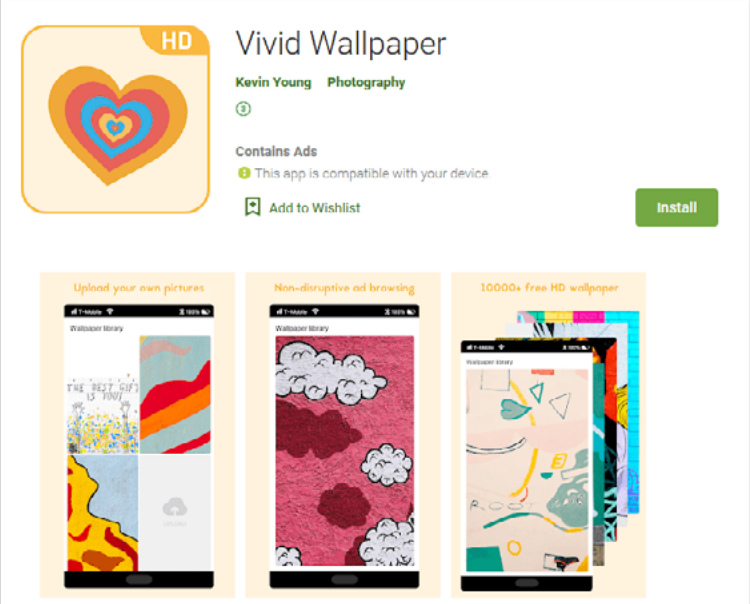
Обзор вирусной активности для мобильных устройств в октябре 2019 года

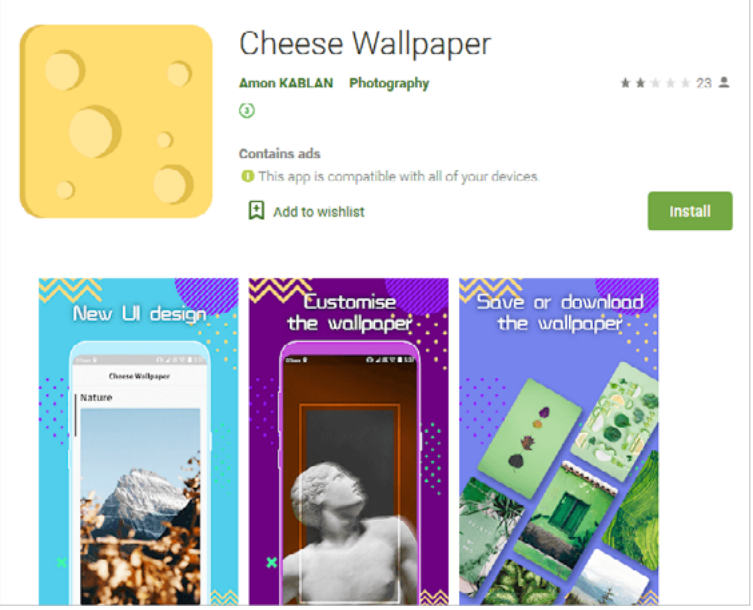
Мобильная угроза месяца



Обзор вирусной активности для мобильных устройств в октябре 2019 года

Мобильная угроза месяца





Обзор вирусной активности для мобильных устройств в октябре 2019 года

По данным антивирусных продуктов Dr.Web для Android

Android.HiddenAds.472.origin

Троянец, показывающий навязчивую рекламу.

Android.RemoteCode.5564

Вредоносное приложение, которое загружает и выполняет произвольный код.

Android.Backdoor.682.origin

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

Android.DownLoader.677.origin

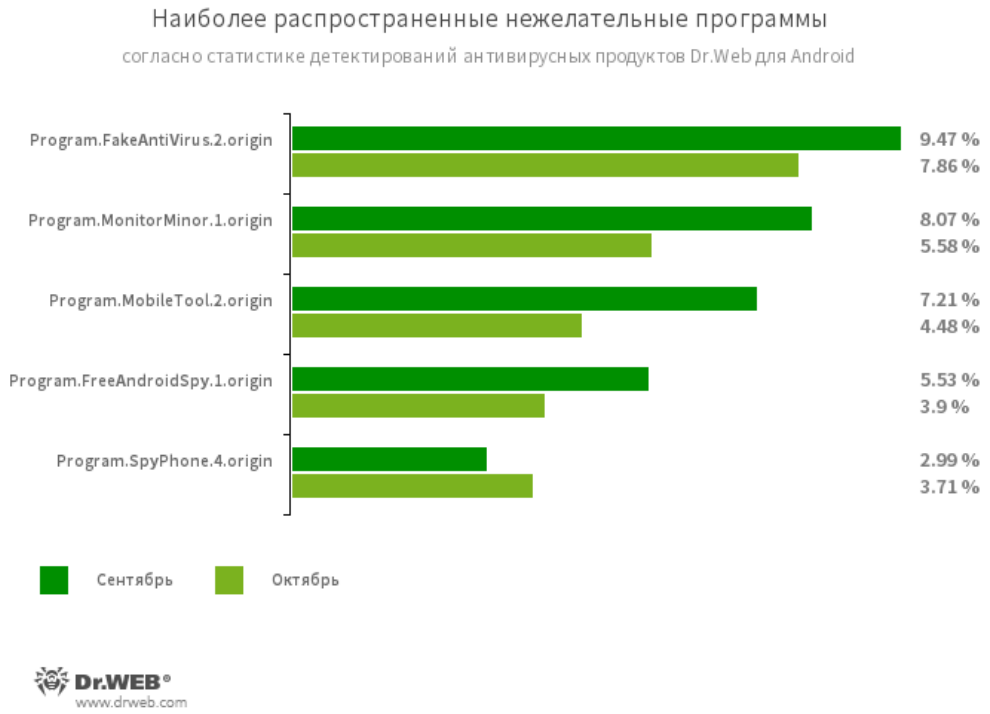
Загрузчик других вредоносных программ.

Android.Triada.465.origin

Многофункциональный троянец, выполняющий разнообразные вредоносные действия.

Обзор вирусной активности для мобильных устройств в октябре 2019 года

По данным антивирусных продуктов Dr.Web для Android



- Program.FakeAntiVirus.2.origin

Детектирование рекламных приложений, которые имитируют работу антивирусного ПО.

- Program.MonitorMinor.1.origin
- Program.MobileTool.2.origin
- Program.FreeAndroidSpy.1.origin
- Program.SpyPhone.4.origin

Программы, которые следят за владельцами Android-устройств и могут использоваться для кибершпионажа.

Обзор вирусной активности для мобильных устройств в октябре 2019 года

По данным антивирусных продуктов Dr.Web для Android

- Tool.SilentInstaller.6.origin
- Tool.SilentInstaller.7.origin
- Tool.SilentInstaller.11.origin
- Tool.VirtualApk.1.origin

Потенциально опасные программные платформы, которые позволяют приложениям запускать apk-файлы без их установки.

- Tool.Rooter.3

Утилита, предназначенная для получения root-полномочий на Android-устройствах. Может использоваться злоумышленниками и вредоносными программами.

Обзор вирусной активности для мобильных устройств в октябре 2019 года

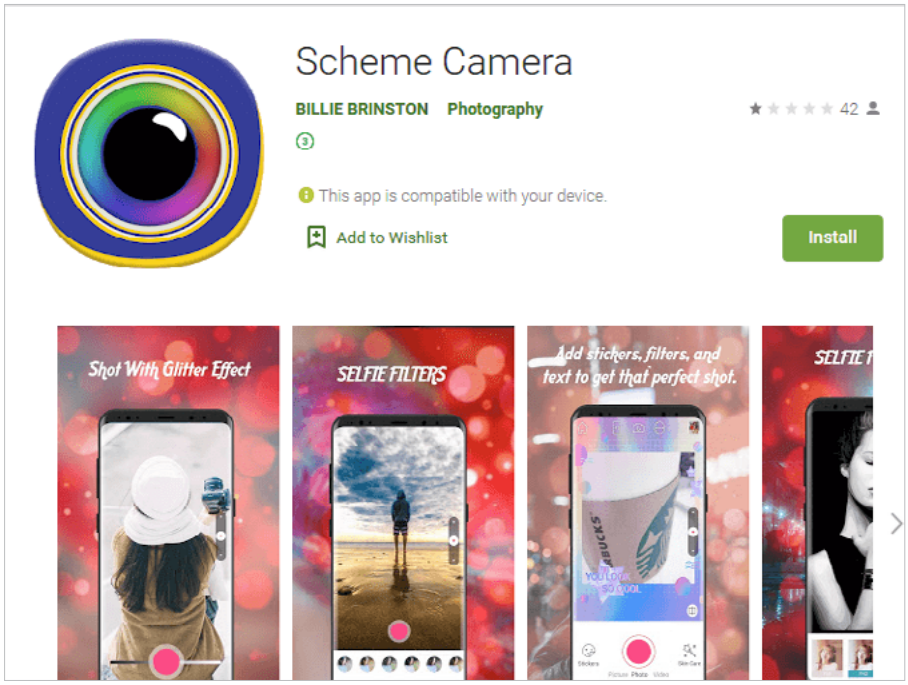
По данным антивирусных продуктов Dr.Web для Android

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

- Adware.Patacore.253
- Adware.Myteam.2.origin
- Adware.Toofan.1.origin
- Adware.Adpush.6547
- Adware.Altamob.1.origin

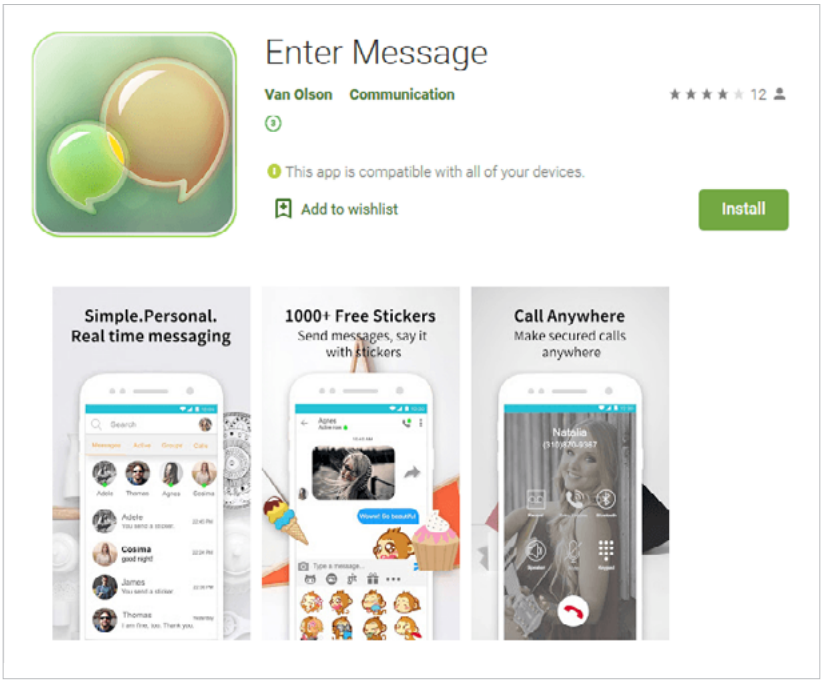
Троянцы в Google Play

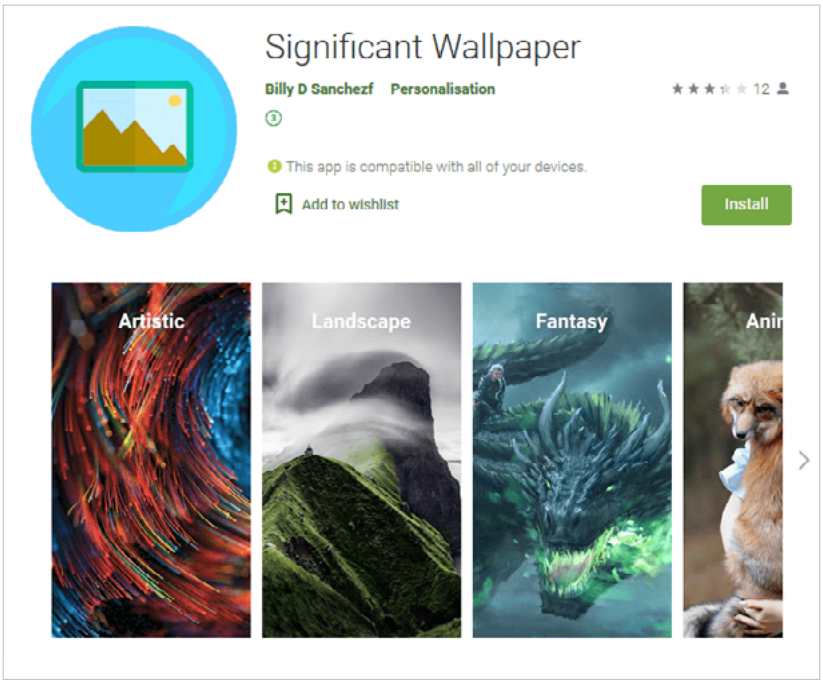
Наряду с троянцами-кликерами вирусные аналитики компании «Доктор Веб» выявили в Google Play множество новых версий, а также модификаций уже известных вредоносных приложений семейства Android.Joker. Среди них — Android.Joker.6, Android.Joker.7, Android.Joker.8, Android.Joker.9, Android.Joker.12, Android.Joker.18 и Android.Joker.20.origin. Эти троянцы загружают и запускают дополнительные вредоносные модули, способны выполнять произвольный код и подписывают пользователей на дорогостоящие мобильные сервисы. Они распространяются под видом полезных и безобидных программ — сборников изображений для рабочего стола, фотокамер с художественными фильтрами, различных утилит, фоторедакторов, игр, интернет-мессенджеров и другого ПО.



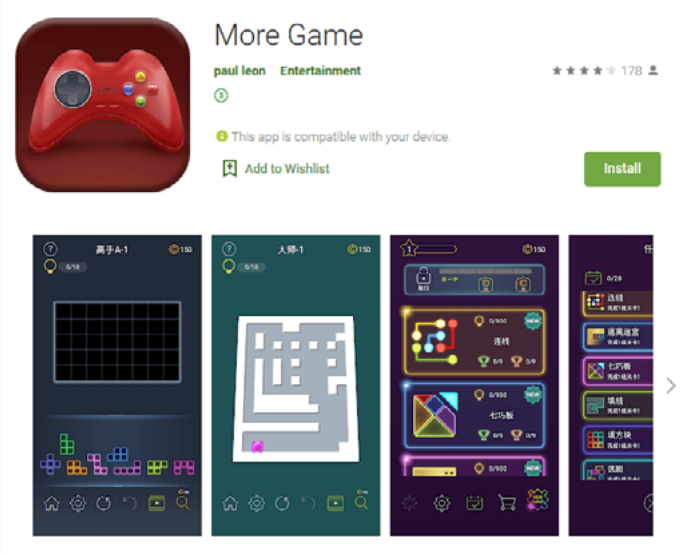
Обзор вирусной активности для мобильных устройств в октябре 2019 года

Троянцы в Google Play



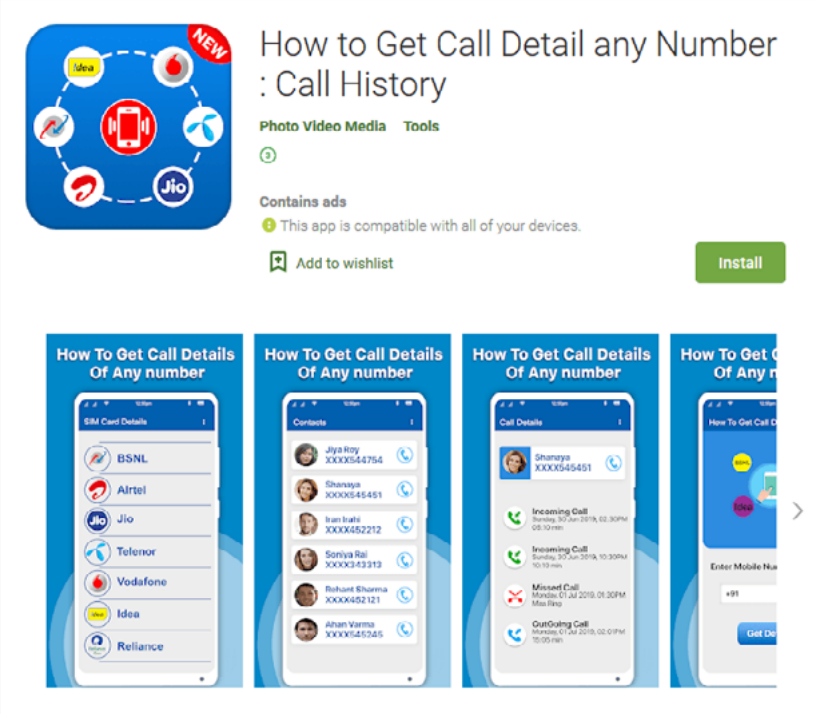


Трояны в Google Play



Кроме того, наши специалисты обнаружили очередного рекламного троянца из семейства Android.HiddenAds, который получил имя Android.HiddenAds.477.origin. Злоумышленники распространяли его под видом видеоплеера и приложения, предоставляющего информацию о телефонных вызовах. После запуска троянец скрывал свой значок в списке приложений главного экрана ОС Android и начинал показывать надоедливую рекламу.

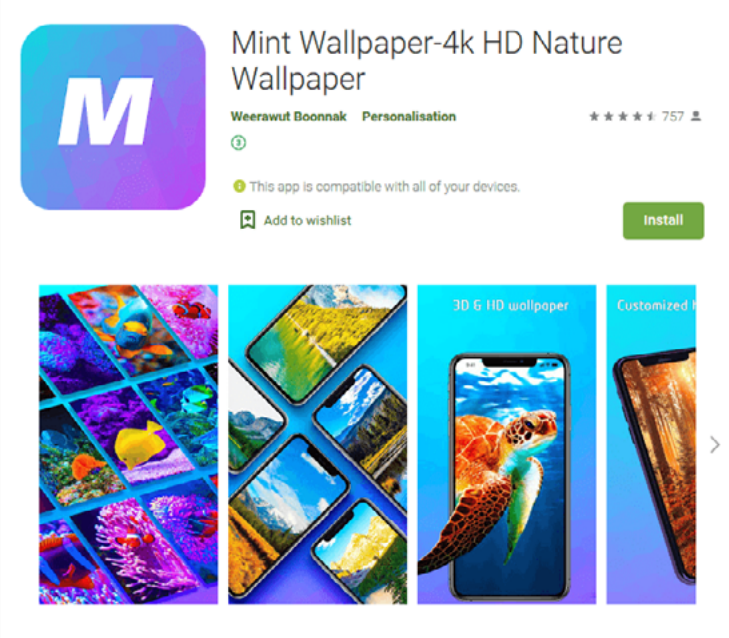
Троянцы в Google Play

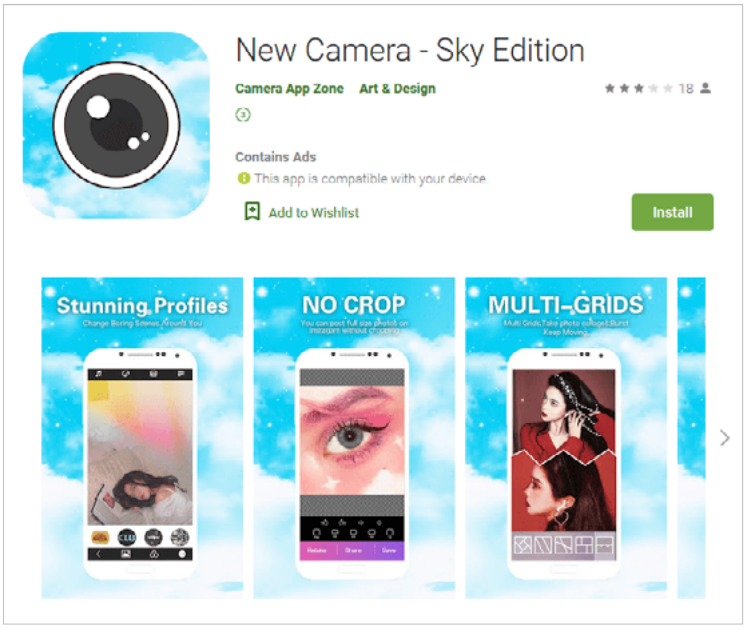


Также в вирусную базу Dr.Web были добавлены записи для детектирования троянцев Android.SmsSpy.10437 и Android.SmsSpy.10447. Они скрывались в сборнике изображений и приложении-фотокамере. Обе вредоносные программы перехватывали содержимое входящих СМС-сообщений, при этом Android.SmsSpy.10437 мог выполнять загружаемый с управляющего сервера произвольный код.

Обзор вирусной активности для мобильных устройств в октябре 2019 года

Троянцы в Google Play





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

Обзор вирусной активности для мобильных устройств в октябре 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.drweb.ru | www.антивирус.рф | free.drweb.ru | www.av-desk.ru
«Доктор Веб» в других странах