Dr.WEB®
с 1992 года

# Обзор вирусной активности за февраль 2015 года

# Обзор вирусной активности за февраль 2015 года

4 марта 2015 года

Самый короткий месяц в году не обошелся без появления новых вредоносных программ. В начале февраля специалисты «Доктор Веб» завершили исследование сложного многофункционального троянца, угрожающего пользователям ОС Linux, а уже в конце месяца были опубликованы результаты изучения новой версии бэкдора для Mac OS X. Также в течение февраля 2015 года были по-прежнему активны вредоносные программы для мобильной платформы Google Android.

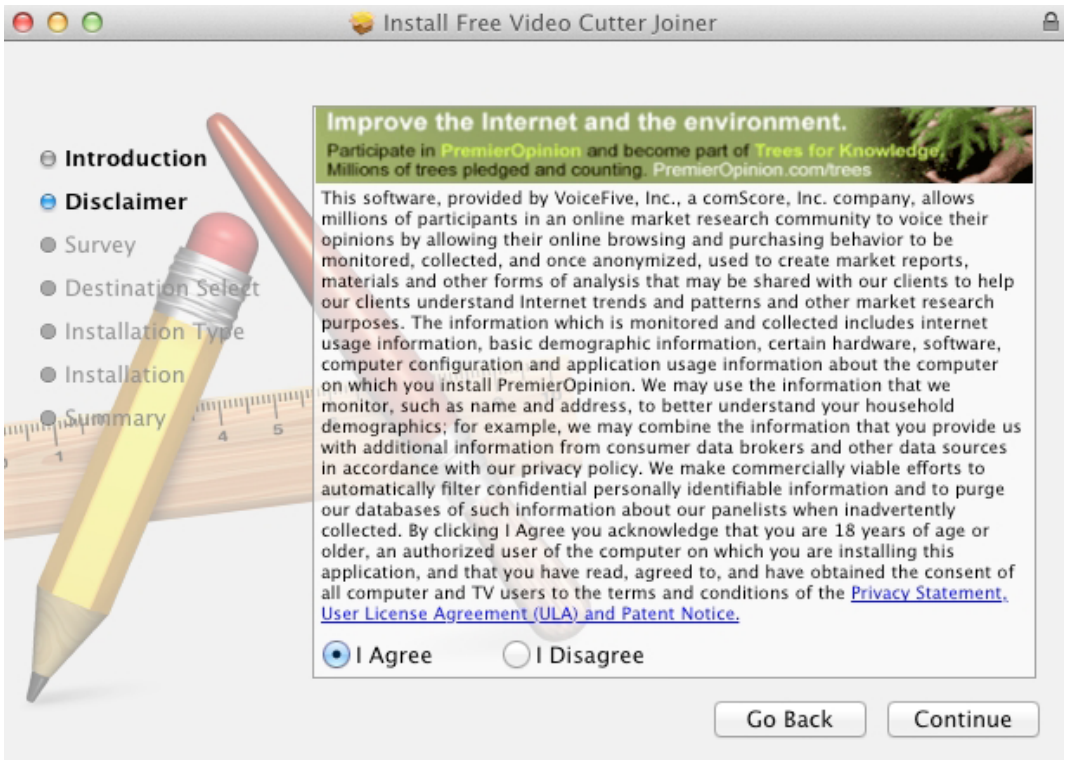
## Главные тенденции февраля

- Появление новых троянских программ для ОС Linux.
- Вирусописатели по-прежнему проявляют интерес к Mac OS X.
- Продолжают распространяться новые вредоносные программы для мобильной платформы Google Android.

# Обзор вирусной активности за февраль 2015 года

## Угроза месяца

В конце февраля специалисты компании «Доктор Веб» завершили исследование трояна-бэкдора Mac.BackDoor.OpinionSpy.3, позволявшего злоумышленникам шпионить за пользователями Mac OS X. Троянец распространялся на сайтах, предлагавших загрузку бесплатного ПО вместе с вполне безобидными приложениями, в дистрибутив которых был встроен дополнительный исполняемый файл. Запустившись в процессе инсталляции с правами администратора, данная программа загружала, устанавливала и запускала на компьютере Apple вредоносное приложение.




Данная вредоносная программа успешно детектируется и удаляется Антивирусом Dr.Web для Mac OS X. Более подробная информация об этом бэкдоре опубликована в соответствующей информационной статье.

# Обзор вирусной активности за февраль 2015 года

Количество добавленных в вирусные базы записей для вредоносных программ, угрожающих пользователям операционной системы Mac OS X.

| Январь 2015 | Февраль 2015 | Динамика |
|---|---|---|
| 9 | 15 | +66,6% |

## Троянцы-шифровальщики

Количество запросов на расшифровку, поступивших в службу технической поддержки «Доктор Веб»

| Январь 2015 | Февраль 2015 | Динамика |
|---|---|---|
| 1305 | 1840 | +40,9% |

Троянцы-энкодеры, шифрующие файлы на компьютерах пользователей и требующие денежный выкуп за их расшифровку, по-прежнему представляют серьезную опасность.

### Наиболее распространенные шифровальщики в феврале 2015 года:

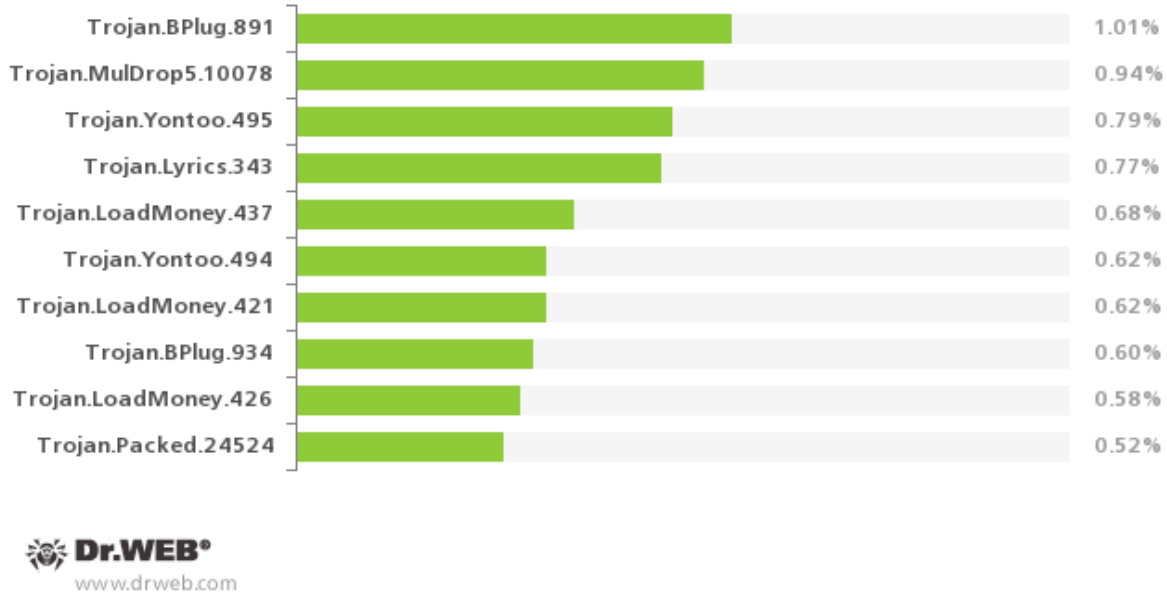
- Trojan.Encoder.567;
- Trojan.Encoder.398;
- Trojan.Encoder.741.

*Защитить владельцев персональных компьютеров от действия троянцев-шифровальщиков может своевременное резервное копирование данных, разумное разделение прав пользователей операционной системы, и, безусловно, современная антивирусная система защиты. Эффективными инструментами противодействия шифровальщикам обладает* ***Dr.Web Security Space версии 10.0****, который включает специальные компоненты превентивной защиты данных от действия троянцев-вымогателей.*

# Обзор вирусной активности за февраль 2015 года

## По данным статистики лечащей утилиты Dr.Web CureIt!

Наиболее распространенные вредоносные программы согласно статистике лечащей утилиты Dr.Web CureIt!



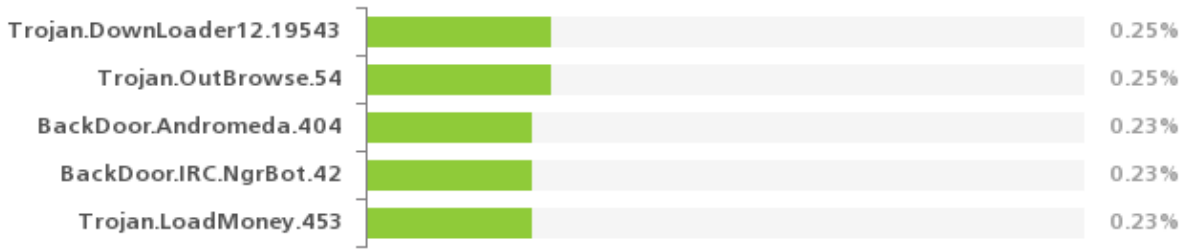

- **Trojan.BPlug**
  Это надстройки (плагины) для популярных браузеров, демонстрирующие назойливую рекламу при просмотре веб-страниц.
- **Trojan.MulDrop5.10078**
  Устанавливает на инфицированный компьютер различные нежелательные и рекламные приложения.
- **Trojan.Yontoo**
  Семейство надстроек для популярных браузеров, назначение которых заключается в демонстрации пользователю рекламы при просмотре веб-страниц.
- **Trojan.Lyrics**
  Семейство троянцев, способных демонстрировать на экране назойливую рекламу и открывать в окне браузера веб-сайты сомнительного содержания без ведома пользователя.

# Обзор вирусной активности за февраль 2015 года

- **Trojan.LoadMoney**
  Семейство программ-загрузчиков, генерируемых серверами партнерской программы LoadMoney. Данные приложения загружают и устанавливают на компьютер жертвы различное нежелательное ПО.
- **Trojan.Packed.24524**
  Троянец-установщик рекламных и нежелательных приложений.

## По данным серверов статистики «Доктор Веб»

Наиболее распространенные вредоносные программы в феврале2015 года согласно данным серверов статистики Dr.Web




Dr.WEB®
www.drweb.com

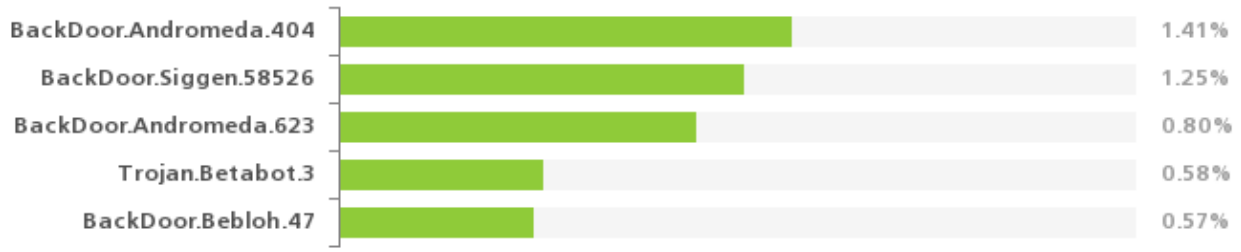
- **Trojan.DownLoader12.19543**
  Троянец, предназначенный для подмены в окне браузера результатов выдачи поисковых систем, а также демонстрации поддельных всплывающих сообщений социальных сетей.
- **Trojan.OutBrowse.54**
  Один из представителей семейства рекламных троянцев, распространяющихся с использованием партнерских программ и предназначенных для монетизации файлового трафика.
- **BackDoor.Andromeda.404**
  Троянец-загрузчик, предназначенный для скачивания с удаленных серверов злоумышленников и запуска на инфицированном компьютере других вредоносных программ.

# Обзор вирусной активности за февраль 2015 года

- **BackDoor.IRC.NgrBot.42**
  Довольно распространенный троянец, известный специалистам по информационной безопасности еще с 2011 года. Вредоносные программы этого семейства способны выполнять на инфицированном компьютере поступающие от злоумышленников команды, а управление ими киберпреступники осуществляют с использованием протокола обмена текстовыми сообщениями IRC (Internet Relay Chat).
- **Trojan.LoadMoney**
  Семейство программ-загрузчиков, генерируемых серверами партнерской программы LoadMoney. Данные приложения загружают и устанавливают на компьютер жертвы различное нежелательное ПО.

# Статистика вредоносных программ в почтовом трафике

Наиболее распространенные вредоносные программы, выявленные в почтовом трафике в феврале 2015 года




Dr.WEB®
www.drweb.com

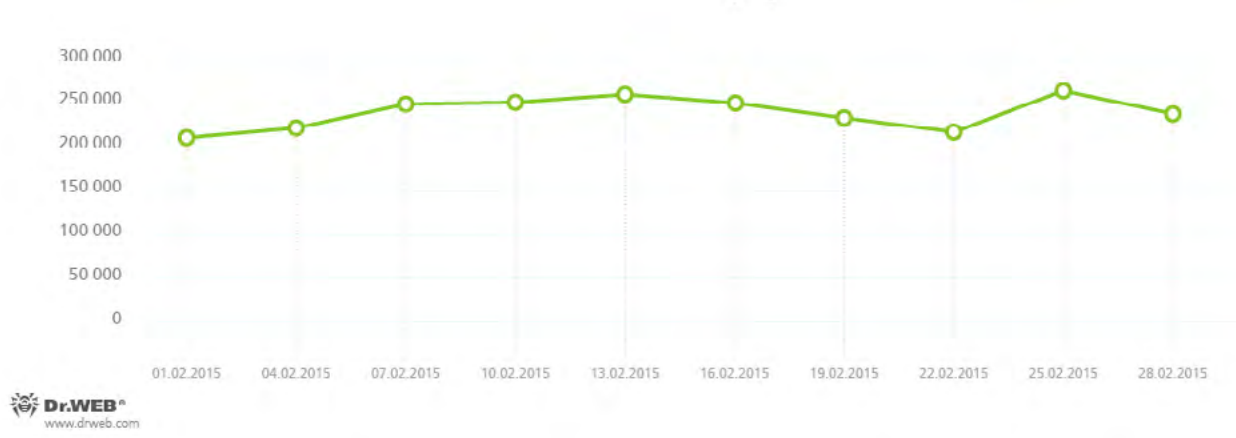
- **BackDoor.Andromeda**
  Семейство троянцев-загрузчиков, предназначенных для скачивания с удаленных серверов злоумышленников и запуска на инфицированном компьютере других вредоносных программ.
- **BackDoor.Siggen.58526**
  Троянец, без ведома пользователей загружающий и запускающий на инфицированном компьютере другие вредоносные программы, а также способный выполнять поступающие от злоумышленников команды.

- **Trojan.Betabot.3**
  Троянец, способный похищать вводимые в веб-формы данные (в том числе в системах «Банк-клиент»), выполнять поступающие с удаленного сервера команды, менять настройки DNS на инфицированном компьютере и проводить DDoS-атаки.
- **BackDoor.Bebloh.47**
  Один из представителей семейства вредоносных программ, относящихся к категории банковских троянцев. Данное приложение представляет угрозу для пользователей систем дистанционного банковского обслуживания (ДБО), поскольку позволяет злоумышленникам красть конфиденциальную информацию путем перехвата заполняемых в браузере форм и встраивания в страницы сайтов некоторых банков.

## Ботнеты

Несмотря на то, что, по сообщениям многочисленных информационных агентств, 24 февраля 2015 года общими усилиями ряда организаций были отключены командные серверы бот-сети **Rmnet**, специалисты компании «Доктор Веб» в целом не наблюдают существенного снижения активности данного ботнета. Так, активность отслеживаемых компанией «Доктор Веб» подсетей ботнета, созданного злоумышленниками и использованием файлового вируса **Win32.Rmnet.12**, представлена на следующих графиках:

Активность ботнета Win32.Rmnet.12 в феврале 2015 года (1 подсеть)



Активность ботнета Win32.Rmnet.12 в феврале 2015 года (2 подсеть)


Более подробную информацию о деятельности ботнета Rmnet можно узнать из опубликованного на нашем сайте информационного материала

Продолжает действовать ботнет, созданный злоумышленниками с использованием файлового вируса Win32.Sector:

Активность ботнета Win32.Sector в феврале 2015 года

# Обзор вирусной активности за февраль 2015 года

## Файловый вирус Win32.Sector реализует следующие функции:

- загрузка из P2P-сети и запуск на зараженной машине различных исполняемых файлов;
- встраивание в запущенные на инфицированном компьютере процессы;
- возможность останавливать работу некоторых антивирусных программ и блокировать доступ к сайтам их разработчиков;
- инфицирование файловых объектов на локальных дисках и сменных носителях (где в процессе заражения создает файл автозапуска autorun.inf), а также файлов, хранящиеся в общедоступных сетевых папках.

Активность ботнета BackDoor.Flashback. в феврале 2015 года


### BackDoor.Flashback.39

Троянская программа для Mac OS X, получившая распространение в апреле 2012 года. Заражение осуществлялось с использованием уязвимостей Java. Предназначение трояна — загрузка и запуск на инфицированной машине полезной нагрузки, в качестве которой может выступать любой исполняемый файл, указанный в полученной троянцем от злоумышленников директиве.

## Угрозы для Linux

Не снижается интерес злоумышленников и к операционным системам семейства Linux. Так, в начале февраля специалисты компании «Доктор Веб» исследовали сложного многофункционального троянца для ОС Linux, получившего наименование Linux.BackDoor.Xnote.1. Эта вредоносная программа умеет выполнять следующие команды для работы с файловой системой, поступающие от злоумышленников:

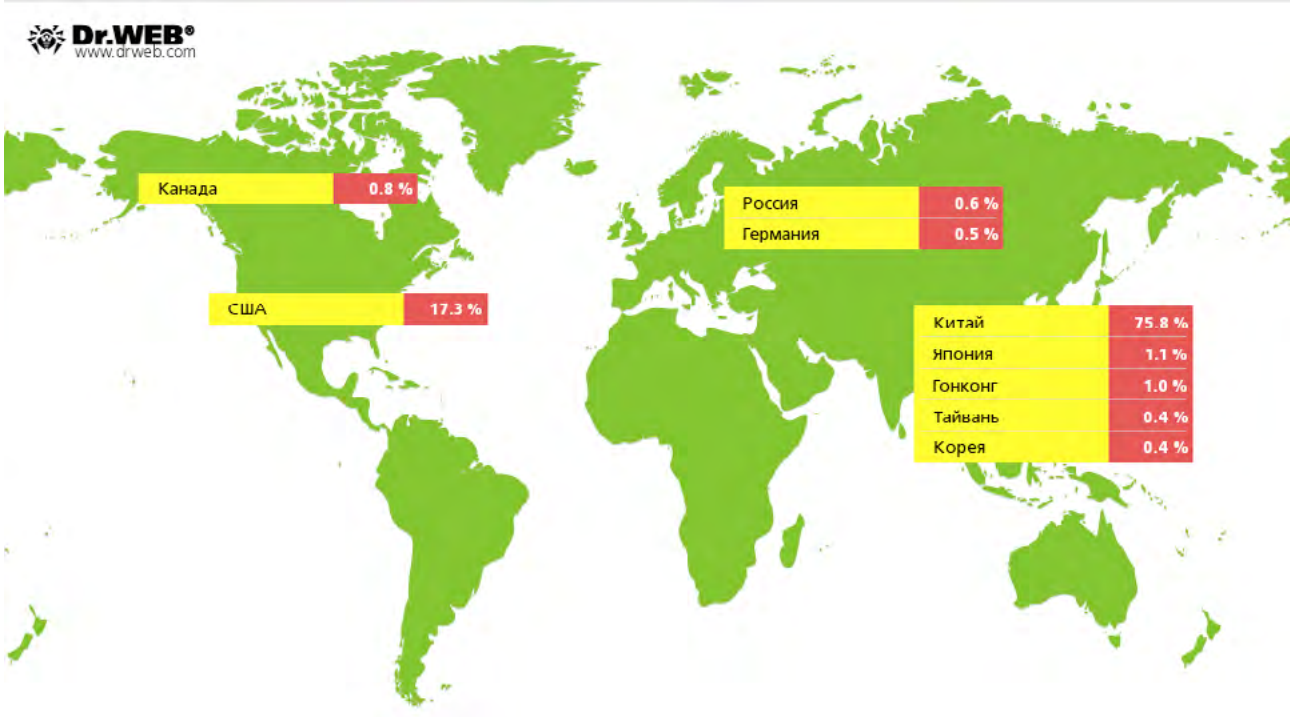
- перечислить файлы и каталоги внутри указанного каталога;
- отослать на сервер сведения о размере файла;
- создать файл, в который можно будет сохранить принимаемые данные;
- принять файл;
- отправить файл на управляющий сервер;
- удалить файл;
- удалить каталог;
- отправить управляющему серверу сигнал о готовности принять файл;
- создать каталог;
- переименовать файл;
- запустить файл.

Кроме того, троянец может запустить командную оболочку (shell) с заданными переменными окружения и предоставить управляющему серверу доступ к ней, запустить на зараженном компьютере SOCKS proxy или собственную реализацию сервера portmap, а также осуществлять DDoS-атаки.

Более подробную информацию о способах распространения и принципах работы Linux.BackDoor.Xnote.1 можно почерпнуть, ознакомившись с опубликованным компанией «Доктор Веб» информационным материалом.

# Обзор вирусной активности за февраль 2015 года

Все так же проявляет активность Linux-троянец **Linux.BackDoor.Gates.5**, продолжающий осуществлять DDoS-атаки на различные сайты в сети Интернет. В феврале 2015 года было выявлено 1129 уникальных IP-адресов, на которые осуществлялись атаки, что на 3880 меньше, чем в прошлом месяце. Как и прежде, большинство из них расположено на территории Китая:



# Обзор вирусной активности за февраль 2015 года

## Мошеннические и нерекомендуемые сайты

*Для защиты пользователей от различных способов мошенничества в Интернете служит компонент Родительский контроль, входящий в комплект поставки Dr.Web Security Space 10.0. Родительский контроль позволяет ограничивать доступ к интернет-сайтам определенной тематики, осуществляет фильтрацию подозрительного контента, а также, используя базы нерекомендуемых ссылок, защищает пользователя от мошеннических, потенциально опасных сайтов, шокирующего контента и ресурсов, замеченных в распространении вредоносного ПО.*

**В течение января 2015 года в базу нерекомендуемых сайтов Dr.Web был добавлен 22 033 интернет-адрес.**

| Январь 2015 | Февраль 2015 | Динамика |
|---|---|---|
| 10 431 | 22 033 | +111,2% |

Узнайте больше о нерекомендуемых Dr.Web сайтах

## Вредоносное и нежелательное ПО для Android

В феврале было выявлено большое число разнообразных вредоносных и потенциально опасных программ для мобильной платформы Google Android, таких как:

- Агрессивные рекламные модули
- Троянцы-вымогатели
- СМС-троянцы
- Троянцы-банкеры

# Обзор вирусной активности за февраль 2015 года

- **Рекламные модули**
  В прошедшем месяце вновь актуальной стала проблема активного применения разработчиками Android-приложений различных агрессивных рекламных систем. В очередной раз подобные программы были выявлены в каталоге Google Play, откуда их скачало несколько десятков миллионов пользователей.
- **Троянцы-вымогатели**
  Среди обнаруженных в феврале вредоносных приложений оказалось немало новых троянцев-вымогателей, в том числе и чрезвычайно опасные вымогатели-энкодеры, шифрующие пользовательские файлы.
- **СМС-троянцы**
  В феврале вирусная база Dr.Web пополнилась большим количеством новых записей для СМС-троянцев, без ведома пользователей отправляющих дорогостоящие сообщения на платные номера.
- **Троянцы-банкеры**
  Распространение банковских вредоносных приложений по-прежнему остается актуальной угрозой для пользователей ОС Android. В частности, под ударом киберпреступников вновь оказались южнокорейские владельцы Android-устройств: для заражения их смартфонов и планшетов злоумышленники организовали более 80 спам-кампаний, рассылая СМС-сообщения со ссылкой на загрузку Android-троянцев.
- **Угрозы в каталоге Google Play**
  Агрессивные и потенциально опасные рекламные платформы для мобильных устройств остаются актуальной проблемой. Одна из таких систем была внедрена в ряде бесплатных программ, размещенных в каталоге Google Play.

УЗНАЙТЕ БОЛЕЕ ПОДРОБНУЮ ИНФОРМАЦИЮ О ВРЕДОНОСНЫХ ПРОГРАММАХ ДЛЯ МОБИЛЬНОЙ ПЛАТФОРМЫ Google Android, ОЗНАКОМИВШИСЬ С НАШИМ СПЕЦИАЛЬНЫМ ОБЗОРОМ.

# Обзор вирусной активности за февраль 2015 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
125124, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп.12а
www.антивирус.рф | www.drweb.ru | www.mobi.drweb.com | www.av-desk.ru
«Доктор Веб» в других странах