Dr.WEB®
с 1992 года

Обзор вирусной активности в июне 2017 года

Обзор вирусной активности в июне 2017 года

3 июля 2017 года

Самым заметным событием первого летнего месяца 2017 года стала эпидемия червя-шифровальщика Trojan.Encoder.12544, упоминаемого в СМИ как Petya, Petya.A, ExPetya и WannaCry-2. Эта вредоносная программа заразила компьютеры множества организаций и частных лиц в различных странах мира. В начале июня вирусные аналитики «Доктор Веб» исследовали две вредоносные программы для Linux. Одна из них устанавливает на инфицированном устройстве приложение для добычи криптовалют, вторая — запускает прокси-сервер. В середине месяца был обнаружен еще один троянец-майнер, но в этом случае он угрожал пользователям ОС Windows. Также в июне было выявлено несколько новых вредоносных программ для мобильной платформы Android.

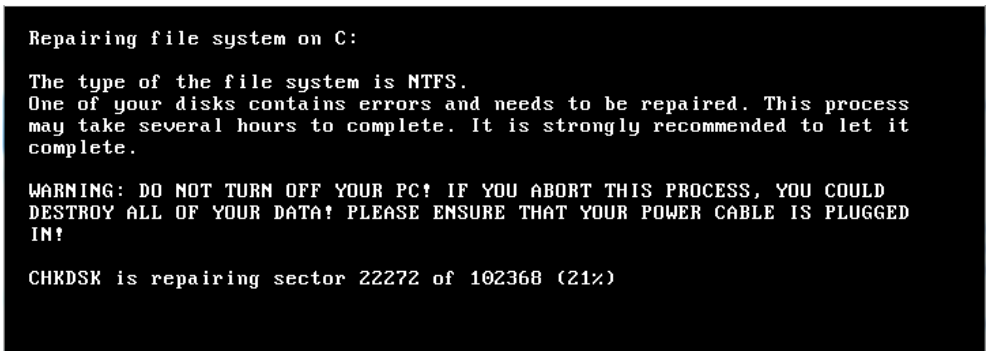
Главные тенденции июня

- Эпидемия червя-шифровальщика Trojan.Encoder.12544
- Распространение троянца-майнера для Windows
- Обнаружение новых вредоносных программ для ОС Linux

Угроза месяца

В первой половине дня 27 июня появились первые сообщения о распространении опасного червя-шифровальщика, которого пресса окрестила Petya, Petya.A, ExPetya и WannaCry-2. Аналитики «Доктор Веб» назвали его Trojan.Encoder.12544. На самом деле с троянцем Petya (Trojan.Ransom.369) у этой вредоносной программы общего не много: схожа лишь процедура шифрования файловой таблицы. Троянец заражает компьютеры при помощи того же набора уязвимостей, которые ранее злоумышленники использовали для внедрения троянца WannaCry. Trojan.Encoder.12544 получает список локальных и доменных пользователей, авторизованных на зараженном компьютере. Затем он ищет доступные на запись сетевые папки, пытается открыть их с использованием полученных учетных данных и сохранить там свою копию. Некоторые исследователи утверждали, что для предотвращения запуска шифровальщика достаточно создать в папке Windows файл perfc, но это не так. Червь действительно выполняет проверку своего повторного запуска по наличию в системной папке файла с именем, соответствующим имени троянца без расширения, но **стоит злоумышленникам изменить исходное имя троянца, и создание в папке C:\Windows\ файла с именем perfc без расширения (как советуют некоторые антивирусные компании) уже не спасет компьютер от заражения. Кроме того, троянец осуществляет проверку наличия файла только при наличии у него достаточных привилегий в операционной системе.**

Trojan.Encoder.12544 портит VBR (Volume Boot Record), копирует оригинальную загрузочную запись Windows в другой участок диска, предварительно зашифровав ее с использованием алгоритма XOR, а вместо нее записывает свою. Далее он создает задание на перезагрузку и шифрует файлы на стационарных дисках компьютера. После перезагрузки червь демонстрирует на экране зараженного ПК текст, напоминающий сообщение стандартной утилиты для проверки дисков CHDISK.



В это время Trojan.Encoder.12544 шифрует MFT (Master File Table). Завершив шифрование, Trojan.Encoder.12544 демонстрирует на экране требование злоумышленников об уплате выкупа.

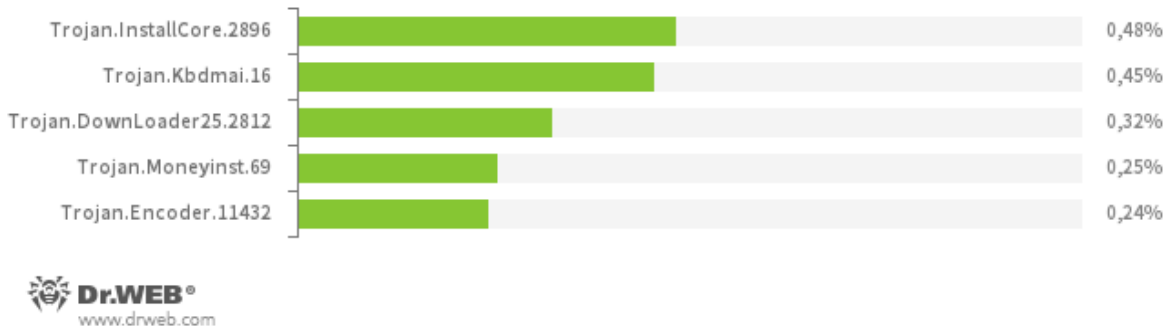
Обзор вирусной активности в июне 2017 года

Вирусные аналитики компании «Доктор Веб» полагают, что Trojan.Encoder.12544 изначально был рассчитан не на получение выкупа, а на уничтожение зараженных компьютеров: во-первых, вирусописатели использовали только один почтовый ящик для обратной связи, который вскоре после начала эпидемии был заблокирован. Во-вторых, ключ, который демонстрируется на экране зараженного компьютера, представляет собой случайный набор символов и не имеет ничего общего с реальным ключом шифрования. В-третьих, передаваемый злоумышленникам ключ не имеет ничего общего с ключом, используемым для шифрования таблицы размещения файлов, поэтому вирусописатели никак не смогут предоставить жертве ключ расшифровки диска. Подробнее о принципах работы Trojan.Encoder.12544 можно прочитать в новостной статье или в техническом описании.

Первоначальным источником распространения троянца была система обновления программы MEDoc – популярного на территории Украины средства ведения налогового учета. Специалисты компании «Доктор Веб» уже знакомы с подобной схемой распространения вредоносных программ. В 2012 году наши вирусные аналитики выявили целенаправленную атаку на сеть российских аптек и фармацевтических компаний с использованием троянца-шпиона BackDoor.Dande. Он похищал информацию о закупках медикаментов из специализированных программ, которые используются в фармацевтической индустрии. Троянец загружался с сайта http://ws.eprica.ru, принадлежащего компании «Спарго Технологии» и предназначенного для обновления программы для мониторинга цен на медикаменты ePrica. Подробнее об этом инциденте рассказано в нашем новостном материале, а детали расследования изложены в техническом описании.

По данным статистики Антивируса Dr.Web

Наиболее распространенные вредоносные программы согласно статистике Антивируса Dr.Web



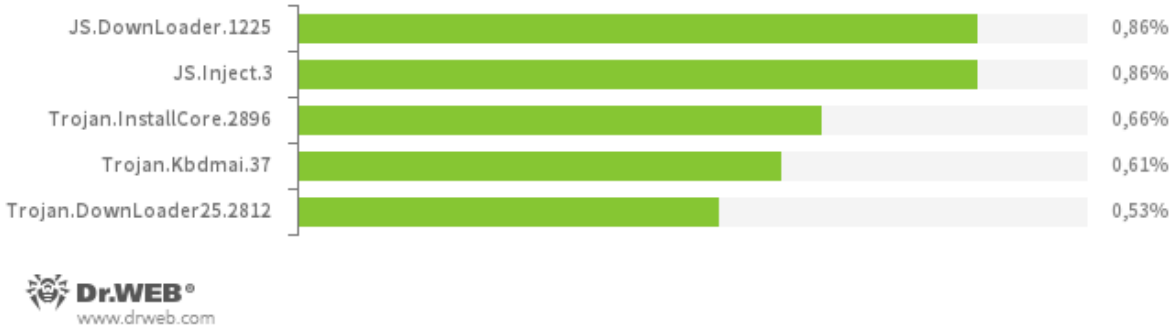
- **Trojan.InstallCore**
  Семейство установщиков нежелательных и вредоносных приложений.

Обзор вирусной активности в июне 2017 года

- **Trojan.Kbdmai.16**
  Представитель семейства рекламных троянцев. Одна из функций этой вредоносной программы – открытие в окне браузера различных веб-сайтов.
- **Trojan.DownLoader**
  Семейство троянцев, предназначенных для загрузки на атакуемый компьютер других вредоносных приложений.
- **Trojan.Moneyinst.69**
  Вредоносная программа, устанавливающая на компьютер жертвы различное ПО, в том числе других троянцев.
- **Trojan.Encoder.11432**
  Сетевой червь, запускающий на компьютере жертвы опасного троянца-шифровальщика. Известен также под именем WannaCry.

По данным серверов статистики «Доктор Веб»

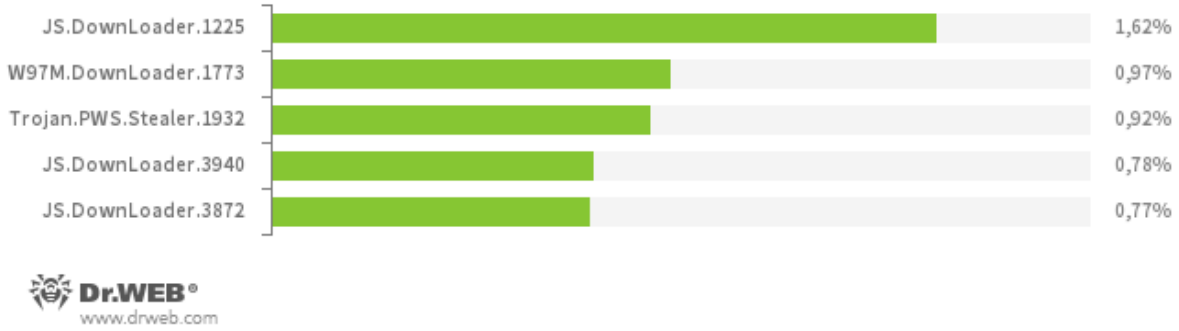
Наиболее распространенные вредоносные программы в июне 2017 года согласно данным серверов статистики Dr.Web



- **JS.DownLoader**
  Семейство вредоносных сценариев, написанных на языке JavaScript. Загружают и устанавливают на компьютер другие вредоносные программы.
- **JS.Inject.3**
  Семейство вредоносных сценариев, написанных на языке JavaScript. Встраивают вредоносный скрипт в HTML-код веб-страниц.
- **Trojan.InstallCore**
  Семейство установщиков нежелательных и вредоносных приложений.
- **Trojan.Kbdmai.37**
  Представитель семейства рекламных троянцев. Одна из функций этой вредоносной программы – открытие в окне браузера различных веб-сайтов.
- **Trojan.DownLoader**
  Семейство троянцев, предназначенных для загрузки на атакуемый компьютер других вредоносных приложений.

Статистика вредоносных программ в почтовом трафике

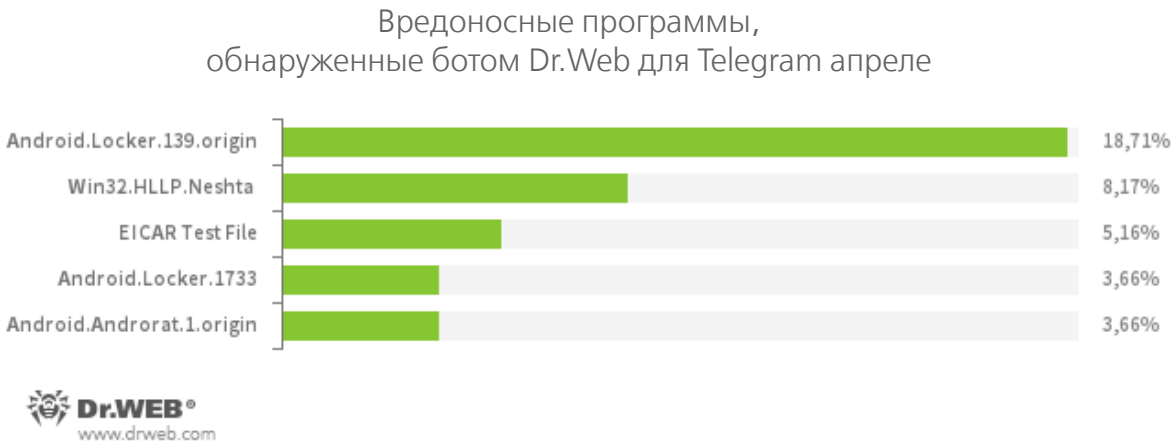
Наиболее распространенные вредоносные программы, выявленные в почтовом трафике в июне 2017 года



- **JS.DownLoader**
  Семейство вредоносных сценариев, написанных на языке JavaScript. Загружают и устанавливают на компьютер другие вредоносные программы.
- **W97M.DownLoader**
  Семейство троянцев-загрузчиков, использующих в работе уязвимости офисных приложений. Предназначены для загрузки на атакуемый компьютер других вредоносных программ.
- **Trojan.PWS.Stealer**
  Семейство троянцев, предназначенных для хищения на инфицированном компьютере паролей и другой конфиденциальной информации.

Обзор вирусной активности в июне 2017 года

По данным бота Dr.Web для Telegram



- **Android.Locker.139.origin, Android.Locker.1733**
  Представители семейства Android-троянцев, предназначенных для вымогательства. Они показывают навязчивое сообщение якобы о нарушении закона и о последовавшей в связи с этим блокировке мобильного устройства, для снятия которой пользователю предлагается заплатить определенную сумму.
- **Win32.HLLP.Neshta**
  Файловый вирус, известный вирусным аналитикам с 2005 года. Заражает файлы EXE PE, размер которых не меньше 41472 байт. При заражении пишет себя в начало инфицированного файла, а оригинальное начало переносит в конец файла. Содержит строчку: «Neshta 1.0 Made in Belarus».
- **EICAR Test File**
  Специальный текстовый файл, предназначенный для тестирования работоспособности антивирусов. Все антивирусные программы при обнаружении такого файла должны реагировать на него в точности таким же образом, как в случае выявления какой-либо реальной компьютерной угрозы.
- **Android.Androrat.1.origin**
  Шпионская программа, работающая на устройствах под управлением ОС Android.

Обзор вирусной активности в июне 2017 года

Трояны-шифровальщики

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

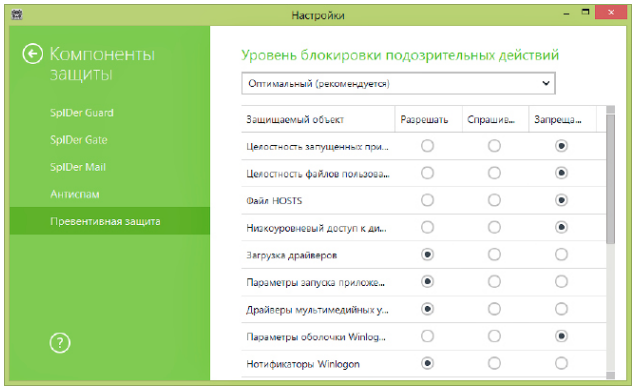
В мае в службу технической поддержки компании «Доктор Веб» чаще всего обращались пользователи, пострадавшие от следующих модификаций троянцев-шифровальщиков:

- **Trojan.Encoder.858** — 28.51% обращений;
- **Trojan.Encoder.10103** — 8.10% обращений;
- **Trojan.Encoder.567** — 5.54% обращений;
- **Trojan.Encoder.11432** — 4.10% обращений;
- **Trojan.Encoder.10144** — 2.36% обращений.

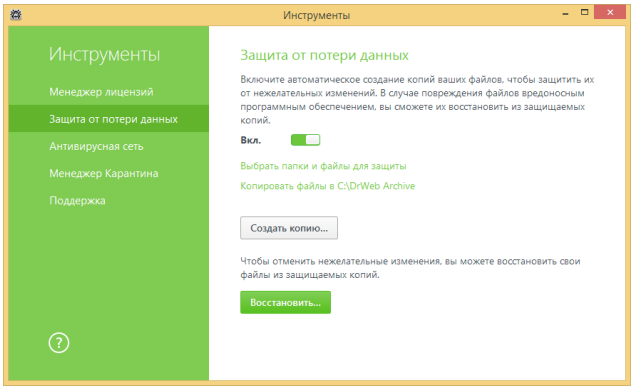
Dr.Web Security Space 11.0 для Windows защищает от троянцев-шифровальщиков

Этого функционала нет в лицензии Антивирус Dr.Web для Windows

Превентивная защита



Защита данных от потери



Подробней Смотрите видео о настройке

Опасные сайты

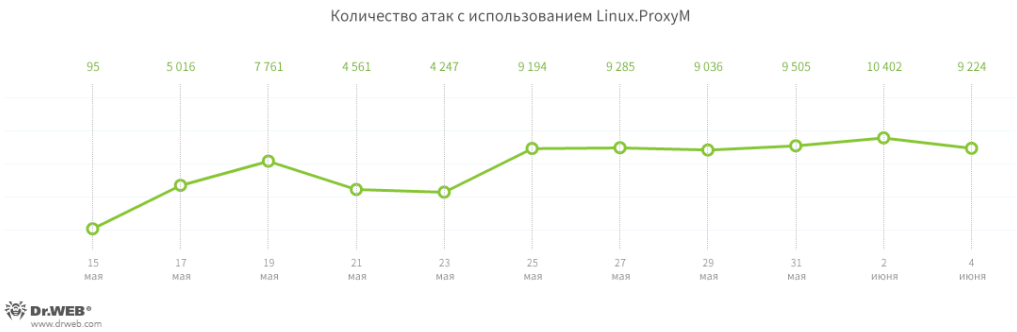
В течение июня 2017 года в базу нерекомендуемых и вредоносных сайтов было добавлено 568 903 интернет-адреса.

Май 2017	Июнь 2017	Динамика
+ 1 129 277	+ 229 381	- 79.68%

Нерекомендуемые сайты

Вредоносные программы для ОС Linux

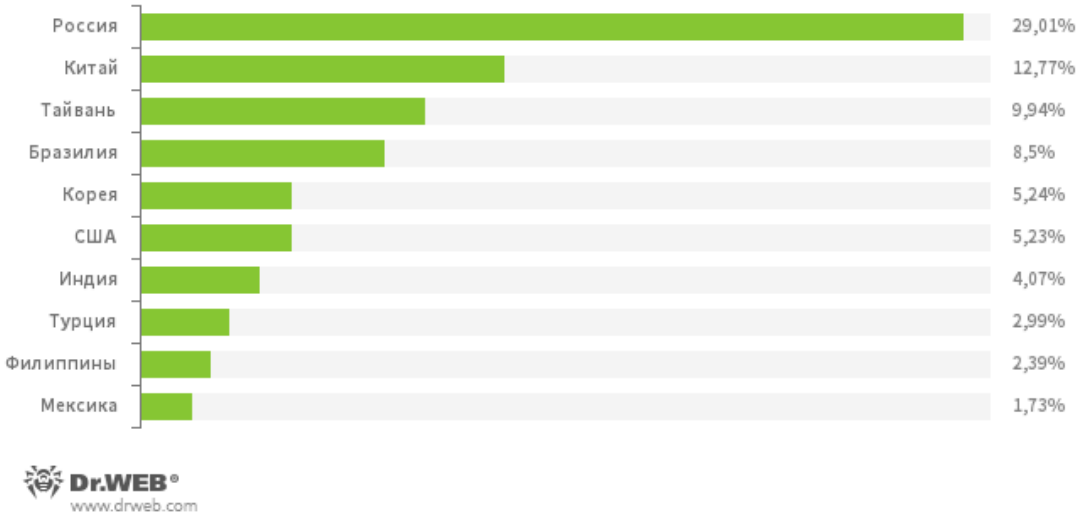
В начале июня вирусные аналитики компании «Доктор Веб» исследовали двух троянцев для ОС Linux. Один из них — Linux.MulDrop.14 — атакует исключительно миникомпьютеры Raspberry Pi. Троянец представляет собой скрипт, в теле которого хранится сжатое и зашифрованное приложение-майнер, которое предназначено для добычи криптовалют. Второй троянец, добавленный в вирусные базы под именем Linux.ProxyM, атаковал пользователей еще с февраля 2017 года, но своего пика атаки достигли во второй половине мая. График зафиксированной специалистами «Доктор Веб» активности троянца Linux.ProxyM представлен ниже.



Значительная часть IP-адресов, с которых осуществляются атаки, расположена на территории России. На втором месте — Китай, на третьем — Тайвань. Распределение источников атак с использованием Linux.ProxyM по географическому признаку показано на следующей иллюстрации:

Обзор вирусной активности в июне 2017 года

Распределение источников атак Linux ProxyM по странам



Другие события в сфере информационной безопасности

Вредоносные программы, которые используют вычислительные ресурсы инфицированных компьютеров для добычи (майнинга) криптовалют, появились вскоре после появления самих криптовалют: первый троянец семейства Trojan.BtcMine был добавлен в вирусные базы Dr.Web в 2011 году. Обнаруженный в июне Trojan.BtcMine.1259 — очередной представитель этого вредоносного семейства. Trojan.BtcMine.1259 предназначен для добычи криптовалюты Monero (XMR). Он скачивается на компьютер троянцем-загрузчиком Trojan.DownLoader24.64313, который, в свою очередь, распространяется с помощью бэкдора DoublePulsar.

Помимо своей основной функции Trojan.BtcMine.1259 расшифровывает и загружает в память хранящуюся в его теле библиотеку, которая представляет собой модифицированную версию системы удаленного администрирования с открытым исходным кодом Gh0st RAT (детектируется Антивирусом Dr.Web под именем BackDoor.Farfli.96). С использованием этой библиотеки злоумышленники могут управлять инфицированным компьютером и выполнять на нем различные команды. Модуль, добывающий криптовалюту Monero (XMR), может загружать расчетами до 80% вычислительных ресурсов зараженной машины. Троянец содержит как 32-, так и 64-разрядную версию майнера. Соответствующая реализация троянца используется на зараженном компьютере в зависимости от разрядности операционной системы. Более подробная информация об архитектуре и принципах работы этого троянца изложена в опубликованной на нашем сайте обзорной статье.

Вредоносное и нежелательное ПО для мобильных устройств

В июне вирусные аналитики «Доктор Веб» обнаружили троянца Android.Spy.377.origin, который атаковал иранских пользователей мобильных устройств. Эта вредоносная программа передавала киберпреступникам конфиденциальную информацию и могла выполнять их команды. Также в июне специалисты «Доктор Веб» выявили в каталоге Google Play потенциально опасные программы, предназначенные для подключения к заблокированным на территории Украины социальным сетям «ВКонтакте» и «Одноклассники». Эти приложения, добавленные в вирусную базу Dr.Web как Program.PWS.1, использовали сервер-анонимайзер для обхода ограничения доступа и не обеспечивали защиту передаваемых данных.

Кроме того, в прошедшем месяце через каталог Google Play распространялись троянцы Android.SmsSend.1907.origin и Android.SmsSend.1908.origin, которые отправляли СМС на платные номера и подписывали пользователей на дорогостоящие услуги. Помимо этого, в вирусную базу были внесены записи для троянцев семейства Android.Dvmap. Эти вредоносные приложения пытались получить root-доступ, заражали системные библиотеки, устанавливали дополнительные компоненты и могли по команде вирусописателей скачивать и запускать ПО без ведома пользователя.

Еще один Android-троянец, обнаруженный в июне, получил имя Android.Encoder.3.origin. Он предназначался для китайских пользователей и после заражения мобильных устройств шифровал файлы на SD-карте, требуя выкуп за их восстановление.

Наиболее заметные события, связанные с «мобильной» безопасностью в июне:

- обнаружение Android-троянца, шпионившего за иранскими пользователями;
- выявление в каталоге Google Play новых угроз;
- распространение троянца-энкодера, который шифровал файлы на карте памяти и требовал выкуп за их расшифровку.

Более подробно о вирусной обстановке для мобильных устройств в июне читайте в нашем обзоре.

Обзор вирусной активности в июне 2017 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