Dr.WEB®
с 1992 года

Обзор вирусной активности в августе 2016 года

Обзор вирусной активности в августе 2016 года

31 августа 2016 года

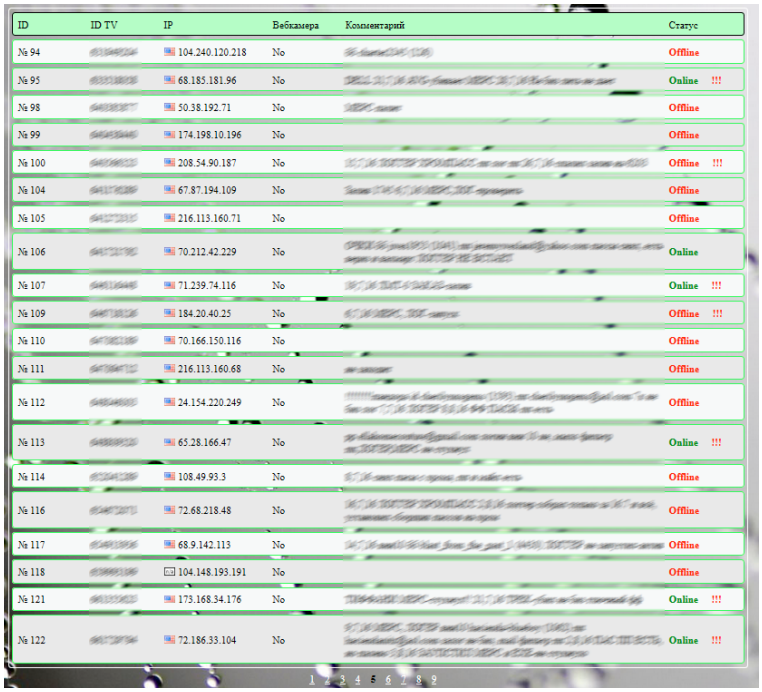
В последний летний месяц аналитики компании «Доктор Веб» исследовали множество вредоносных программ. Еще в начале августа был обнаружен троянец, заражающий POS-терминалы. Чуть позже завершилось исследование двух написанных на языке Go Linux-троянцев, один из которых способен организовывать ботнеты. Была выявлена очередная вредоносная программа, использующая популярную утилиту удаленного администрирования TeamViewer, а также троянец, устанавливающий на компьютеры жертв поддельный браузер.

Главные тенденции августа

- Появление троянца для POS-терминалов
- Распространение новых троянцев для Windows
- Появление троянцев для Linux, написанных на языке Go

Угроза месяца

Вредоносные программы, использующие утилиту TeamViewer, встречаются вирусным аналитикам нередко: об одной из них мы уже рассказывали в мае этого года. Исследованный в августе троянец BackDoor.TeamViewerENT.1 также известен под именем Spy-Agent. В отличие от своих предшественников, BackDoor.TeamViewerENT.1 использует возможности TeamViewer именно для шпионажа за пользователем.



ID	ID TV	IP	Вебкамера	Комментарий	Статус
№ 94		104.240.120.218	No		Offline
№ 95		68.185.181.96	No		Online !!!
№ 98		50.38.192.71	No		Offline
№ 99		174.198.10.196	No		Offline
№ 100		208.54.90.187	No		Offline !!!
№ 104		67.87.194.109	No		Offline
№ 105		216.113.160.71	No		Offline
№ 106		70.212.42.229	No		Online
№ 107		71.239.74.116	No		Online !!!
№ 109		184.20.40.25	No		Offline !!!
№ 110		70.166.150.116	No		Offline
№ 111		216.113.160.68	No		Offline
№ 112		24.154.220.249	No		Offline
№ 113		65.28.166.47	No		Online !!!
№ 114		108.49.93.3	No		Offline
№ 116		72.68.218.48	No		Offline
№ 117		68.9.142.113	No		Offline
№ 118		104.148.193.191	No		Offline
№ 121		173.168.34.176	No		Online !!!
№ 122		72.186.33.104	No		Online !!!

1 2 3 4 5 6 7 8 9

Бэкдор может самостоятельно скачивать со своего управляющего сервера недостающие компоненты TeamViewer и выполнять следующие команды:

- перезагрузить ПК;
- выключить ПК;
- удалить TeamViewer;
- перезапустить TeamViewer;
- начать прослушивание звука с микрофона;
- завершить прослушивание звука с микрофона;
- определить наличие веб-камеры;
- начать просмотр через веб-камеру;

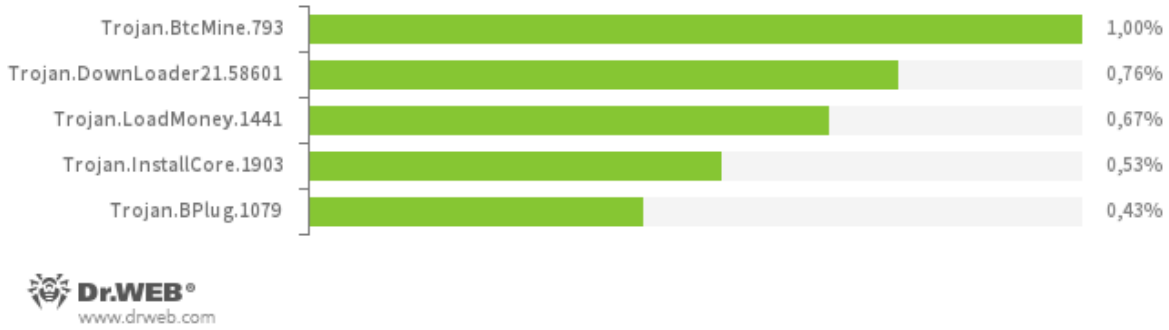
Обзор вирусной активности в августе 2016 года

- завершить просмотр через веб-камеру;
- скачать файл, сохранить его во временную папку и запустить;
- обновить конфигурационный файл или файл бэкдора;
- подключиться к указанному удаленному узлу, после чего запустить cmd.exe с перенаправлением ввода-вывода на удаленный хост.

Вирусные аналитики компании «Доктор Веб» установили, что с использованием BackDoor.TeamViewerENT.1 злоумышленники в различное время атакуют жителей строго определенных стран и регионов. Подробнее о целях этих атак и принципах работы троянца можно узнать из опубликованной на нашем сайте информационной статьи.

По данным статистики лечащей утилиты Dr.Web CureIt!

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

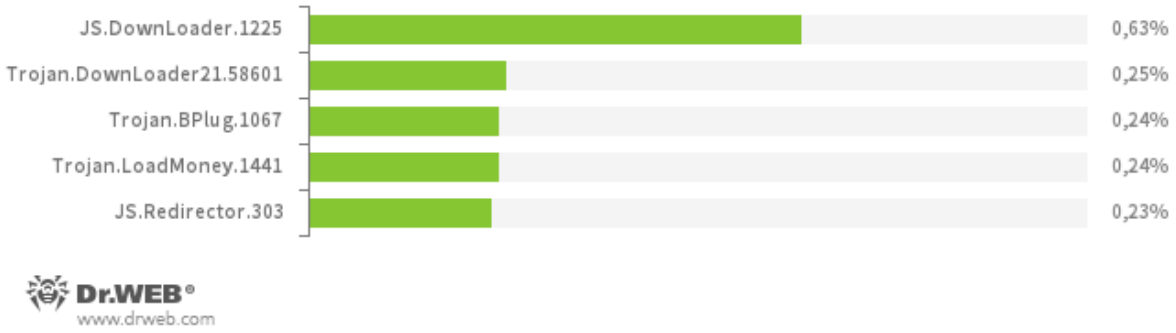


- **Trojan.BtcMine.793**
  Представитель семейства вредоносных программ, предназначенных для негласного использования вычислительных ресурсов зараженного компьютера с целью добычи (майнинга) различных криптовалют, например Bitcoin.
- **Trojan.DownLoader**
  Семейство троянцев, предназначенных для загрузки на атакуемый компьютер других вредоносных приложений.
- **Trojan.InstallCore.1903**
  Представитель семейства установщиков нежелательных и вредоносных приложений.
- **Trojan.BPlug**
  Это надстройки (плагины) для популярных браузеров, демонстрирующие назойливую рекламу при просмотре веб-страниц.

Обзор вирусной активности в августе 2016 года

По данным серверов статистики «Доктор Веб»

Наиболее распространенные вредоносные программы в августе 2016 года
согласно данным серверов статистики Dr.Web

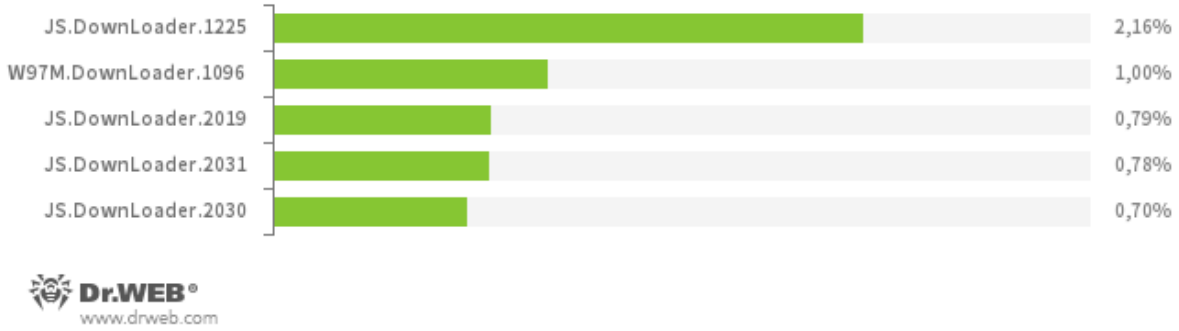


- **JS.Downloader**
  Семейство вредоносных сценариев, написанных на языке JavaScript. Загружают и устанавливают на компьютер другие вредоносные программы.
- **Trojan.DownLoader**
  Семейство троянцев, предназначенных для загрузки на атакуемый компьютер других вредоносных приложений.
- **Trojan.BPlug**
  Это надстройки (плагины) для популярных браузеров, демонстрирующие назойливую рекламу при просмотре веб-страниц.
- **Trojan.LoadMoney**
  Семейство программ-загрузчиков, генерируемых серверами партнёрской программы LoadMoney. Данные приложения загружают и устанавливают на компьютер жертвы различное нежелательное ПО.
- **JS.Redirector**
  Семейство вредоносных сценариев, написанных на языке JavaScript. Автоматически перенаправляют пользователей браузеров на другие веб-страницы.

Обзор вирусной активности в августе 2016 года

Статистика вредоносных программ в почтовом трафике

Наиболее распространенные вредоносные программы, выявленные в почтовом трафике в августе 2016 года



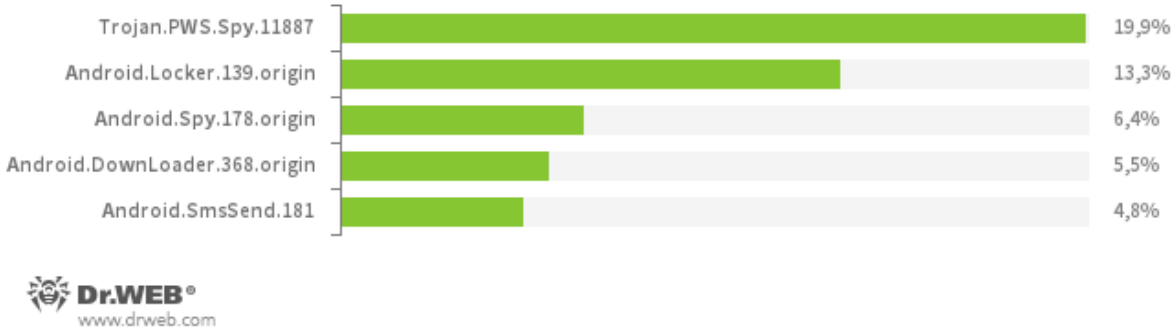
- **JS.Downloader**
  Семейство вредоносных сценариев, написанных на языке JavaScript, предназначенных для загрузки и установки на компьютер других вредоносных программ.
- **W97M.DownLoader**
  Семейство троянцев-загрузчиков, использующих в работе уязвимости офисных приложений. Предназначены для загрузки на атакуемый компьютер других вредоносных программ.

Угроза месяца

В марте 2016 года начал свою работу бот Dr.Web для Telegram. Бот может «на лету» проверить ссылку или файл и вовремя сообщить об угрозе. Например, предупредить о том, что полученный по почте файл является вирусом, или предостеречь от посещения вредоносного веб-сайта. За прошедшие месяцы этой возможностью воспользовалось несколько десятков тысяч человек. Собранная компанией «Доктор Веб» статистика свидетельствует о том, что пользователи Telegram обнаруживают при помощи бота Dr.Web вредоносные программы не только для Microsoft Windows, но и для мобильной платформы Android. Кроме того, в августе 2016 года 5,9% пользователей проверили работу бота с помощью тестового файла EICAR. Топ-5 вредоносных программ, выявленных в августе ботом Dr.Web для Telegram, представлены на диаграмме ниже.

Обзор вирусной активности в августе 2016 года

Вредоносные программы,
обнаруженные ботом Dr.Web для Telegram в августе

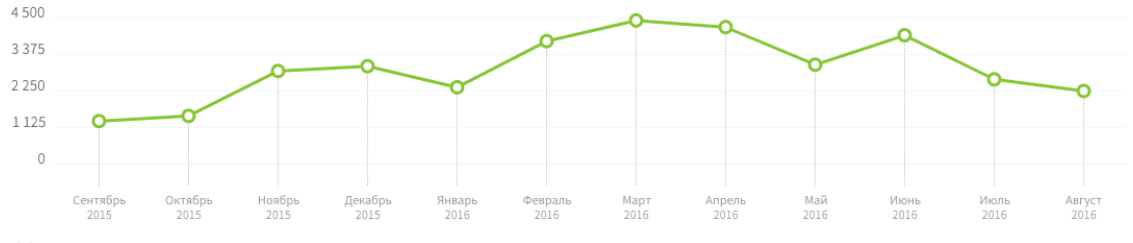


- **Trojan.PWS.Spy**
  Семейство вредоносных программ, которые крадут у пользователей Windows личные данные, например, пароли.
- **Android.Locker**
  Семейство Android-троянцев, предназначенных для вымогательства денег у пользователей. Различные модификации этих вредоносных программ блокируют устройство и показывают сообщение о том, что пользователь якобы нарушил закон. Чтобы снять блокировку, жертве нужно заплатить определенную сумму.
- **Android.Spy**
  Семейство многофункциональных троянцев, поражающих мобильные устройства под управлением ОС Android. Могут читать и записывать контакты, принимать и отправлять СМС-сообщения, определять GPS-координаты, читать и записывать закладки браузера, получать сведения об IMEI мобильного устройства и номере мобильного телефона.
- **Android.DownLoader**
  Троянские программы, предназначенные для загрузки и установки других вредоносных приложений на мобильные устройства под управлением ОС Android.
- **Android.SmsSend**
  Семейство вредоносных программ, работающих на мобильных устройствах под управлением ОС Android. Троянцы этого семейства предназначены для отправки дорогостоящих СМС-сообщений.

Обзор вирусной активности в августе 2016 года

Трояны-шифровальщики

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



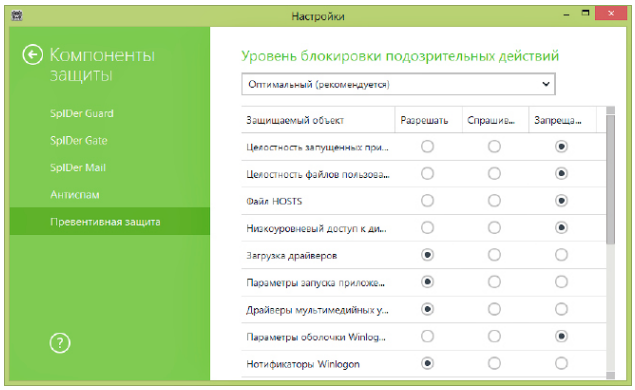
В августе в службу технической поддержки компании «Доктор Веб» чаще всего обращались пользователи, пострадавшие от следующих модификаций троянцев-шифровальщиков:

- **Trojan.Encoder.761** — 17,69% обращений;
- **Trojan.Encoder.858** — 15,40% обращений;
- **Trojan.Encoder.4860** — 12,56% обращений;
- **Trojan.Encoder.567** — 9,49% обращений;
- **Trojan.Encoder.3953** — 6,08% обращений.

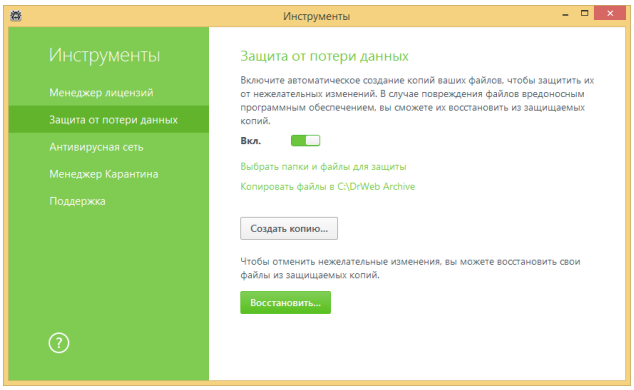
Dr.Web Security Space 11.0 для Windows защищает от троянцев-шифровальщиков

Этого функционала нет в лицензии Антивирус Dr.Web для Windows

Превентивная защита



Защита данных от потери



Подробней Смотрите видео о настройке

Опасные сайты

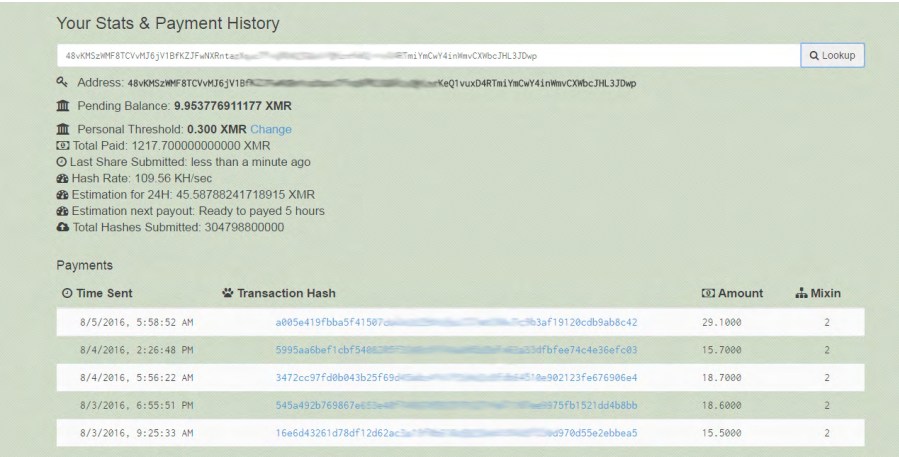
В течение августа 2016 года в базу нерекомендуемых и вредоносных сайтов было добавлено 245 394 интернет-адресов.

Июнь 2016	Июль 2016	Динамика
+ 139 803	+ 245 394	+75,5%

Нерекомендуемые сайты

Вредоносные программы для Linux

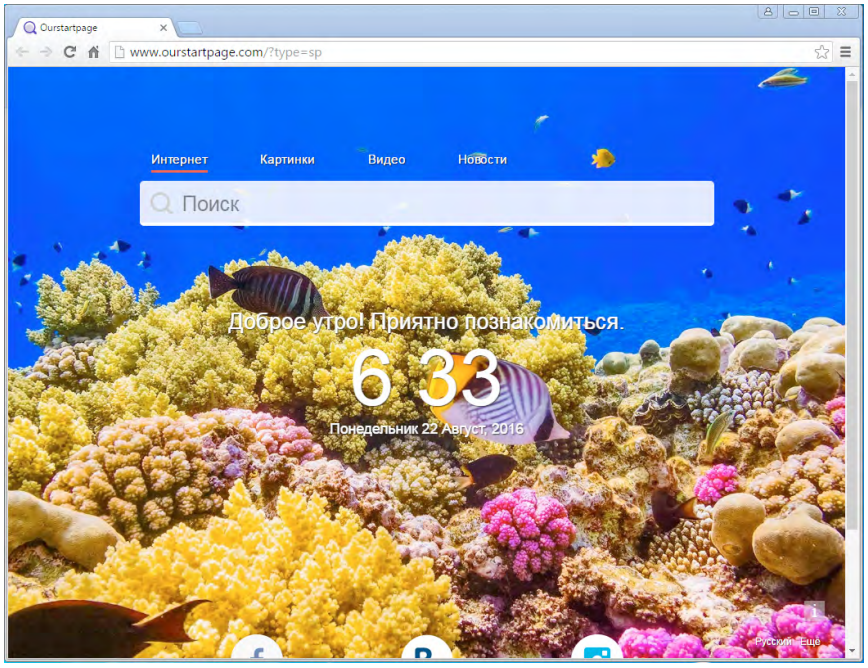
В начале августа вирусные аналитики компании «Доктор Веб» обнаружили троянца для ОС Linux, написанного на языке Go. Эта вредоносная программа получила наименование Linux.Lady.1. Троянец предназначен для загрузки и запуска на зараженном компьютере программы для добычи (майнинга) криптовалют. После запуска Linux.Lady.1 передает на управляющий сервер информацию об установленной на компьютере версии Linux и наименовании семейства ОС, к которой она принадлежит, данные о количестве процессоров, имени, числе запущенных процессов и другие сведения. В ответ троянец получает конфигурационный файл, с использованием которого скачивается и запускается программа-майнер. Полученные деньги перечисляются на электронный кошелек злоумышленников.



Другие события

В начале месяца был обнаружен троянец Trojan.Kasidet.1, заражающий POS-терминалы. Помимо функций троянца для POS-терминалов он может похищать пароли от почтовых программ Outlook, Foxmail или Thunderbird и внедряться в процессы браузеров Mozilla Firefox, Google Chrome, Microsoft Internet Explorer и Maxthon для перехвата GET- и POST-запросов. Также эта вредоносная программа по команде с управляющего сервера может скачать и запустить на зараженном ПК другое приложение или вредоносную библиотеку, найти на дисках и передать злоумышленникам заданный файл или сообщить им список работающих на компьютере процессов. Более подробно читайте о Trojan.Kasidet.1 в нашей обзорной статье.

В конце августа стал распространяться троянец Trojan.Mutabaha.1, который устанавливает на компьютеры жертв поддельный браузер Chrome.



Этот браузер имеет собственное имя — Outfire, однако создатели Trojan.Mutabaha.1 распространяют 56 аналогичных браузеров с различными названиями. Outfire подменяет собой уже установленный в системе браузер Google Chrome — модифицирует имеющиеся ярлыки (или удаляет их и создает новые), а также копирует в новый браузер существующий профиль пользователя Chrome. Стартовую страницу этого браузера нельзя изменить в настройках. Кроме того, он содержит неотключаемый плагин, подменяющий рекламу на веб-страницах страницах, которые просматривает пользователь. Этой вредоносной программе посвящена опубликованная на нашем сайте обзорная статья.

Вредоносное и нежелательное ПО для мобильных устройств

В августе вирусные аналитики компании «Доктор Веб» обнаружили троянца для ОС Android, который показывал надоедливую рекламу поверх запущенных приложений и интерфейса операционной системы, а также мог самостоятельно покупать и загружать программы из каталога Google Play. Кроме того, в прошедшем месяце в онлайн-магазине Apple iTunes были выявлены поддельные программные продукты Dr.Web для iOS.

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

- обнаружение Android-троянца, который показывал навязчивую рекламу и мог автоматически покупать и загружать ПО из каталога Google Play;
- обнаружение в магазине Apple iTunes поддельных приложений Dr.Web для iOS.

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

Обзор вирусной активности в августе 2016 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