Dr.WEB®
Сделано в России

ЗАЩИТИ СОЗДАННОЕ

Путь UNIX

> «В Линуксе не может быть вирусов – миллионы пользователей просматривают код и сразу его найдут! При скачивании нужно просто сравнить diff'ом код старой и новой версии – и вирус будет найден!»
>
> «Линуксоидам бояться нечего: вероятность, что какая-либо зараза проникнет на ваш компьютер, а если даже каким-то образом проникнет, то нанесет ему ощутимый вред, практически нулевая».
>
> *Мнения из Интернета*

Еще недавно любая новость о вредоносной программе, созданной под ОС типа UNIX, на любом форуме приводила к бурному восторгу и просьбам предоставить это ПО с целью попытки его запуска.

> Здравствуйте, я первый и единственный вирус на линуксе.
>
> Если у вас линукс, сотрите, пожалуйста, какой-нибудь файл, который Вы сможете стереть, и разошлите меня по емайлу всем своим друзьям.
>
> Прошу прощения за неудобство, но по-другому распространяться у меня не получается, я пробовал. Поверьте, если бы у меня была хоть одна возможность сделать всё самостоятельно, я бы ни в коем случае не стал бы Вас беспокоить.
>
> Заранее благодарю за понимание и сотрудничество.
>
> P.S. Если Вы будете так добры, что поцарапаете винчестер и разобьёте монитор — я даже стану аппаратным.
>
> Источник

Раньше ежегодное количество создаваемых вредоносных программ для UNIX исчислялось единицами, и встретиться с ними доводилось не каждому. Но год от года число троянцев росло, все чаще стали появляться сообщения о попытках массового заражения серверов или помещения вредоносного кода в репозитории, а то и в код проекта. Активизировались и попытки обнаружения уязвимостей:

- 07.08.2013. уязвимость позволяет организовать выполнение кода на стороне клиента при попытке подключения к серверу злоумышленника.
- 06.08.2013. Возможность восстановить содержимое отдельных секретных идентификаторов (например, сессионные cookie и CSRF-токены), передаваемых внутри зашифрованного HTTPS-соединения.
- 06.08.2013. В поставке OpenX, открытого движка для организации показа online-рекламы, обнаружен бэкдор.
- 05.08.2013. уязвимость, дающая возможность вывести Samba-сервер из строя через инициирование зацикливания операций выделения памяти.
- 01.08.2013. Возможность создания ботнета, построенного из пользовательских браузеров, поражаемых через распространение подставной рекламы в легитимных рекламных сетях.
- 29.07.2013. Зафиксированы факты активной эксплуатации уязвимой конфигурации связки Exim и Dovecot.
- 28.06.2013. Система автоматического тестирования обнаружила, что более 1200 исполняемых файлов ОС Debian Wheezy подвержены потенциальным уязвимостям.
- 03.04.2013. Около двух тысяч серверов, в большинстве своём использующих различные дистрибутивы Linux, оказались жертвами нового вредоносного ПО, оформленного в виде модуля к HTTP-серверу Apache и осуществляющего подстановку вредоносных JavaScript или iframe-блоков

в трафик, отдаваемый сайтами пользователей хостинга. Среди систем на которых был выявлен вредоносный модуль Apache фигурируют серверы, обслуживающие web-ресурсы крупных компаний, таких как Los Angeles Times и Seagate.

- 19.02.2013. Зафиксирован массовый взлом серверов на базе Linux.
- 16.02.2013. В ядре Linux обнаружена уязвимость, которая может быть использована локальным злоумышленником для выполнения кода на уровне ядра.
- 1.09.2011. На серверах kernel.org находился троян, который записывал пароли, действия пользователей, предоставлял root-доступ и модифицировал ПО на сервере.

Только через **17 дней** троян был обнаружен на машине одного из разработчиков ядра H Peter Anvin. Далее на серверах kernel.org Hera и Odin1.

> Одна из существенных причин, почему лично я предпочитаю Linux – это отсутствие вирусов. Не нужен антивирус, ты не боишься до паранойи потерять свои пароли.
>
> В Linux есть свои репозитории, в которых программы защищены.
>
> Источник

- 10.12.2009. В каталоге GNOME-Look зафиксировано наличие вредоносного ПО.
- 13.09.2009. Обнаружен кластер Linux-серверов и занимающийся распространением вредоносного программного обеспечения.

> - ну какое отношение имеет веб ботнет к линуксу?
> - Это проблема дефолтных настроек. Ну никак не линукса!
>
> *Отзывы на форуме*

- 25.01.2008. Заражение компьютеров под управлением Linux с установленным HTTP-сервером Apache.

> Да, вирусы под Linux существуют! Большинство из них существует только как доказательство того факта, что такую программу можно написать в принципе (proof of concept).
>
> *По-прежнему распространенное мнение*

Немногочисленность троянцев, червей и вирусов стала причиной того, что администраторы пренебрегали защитой UNIX-систем. Это наглядно показал эксперимент, в ходе которого исследователи заразили и использовали **420 тысяч** систем – и никто в мире этого не заметил!

> Все СМИ ссылаются на один и тот же источник. На сайт производителя антивирусов Dr. Web. У этого производителя есть платный антивирус для Linux, но нет желающих его покупать, так как сказок про страшные вирусы под Linux много, но сами линуксоиды никогда с ними не сталкивались.
>
> Источник

Критический рубеж был пройден с созданием ботнета Mirai (первый образец был выявлен в феврале 2017).

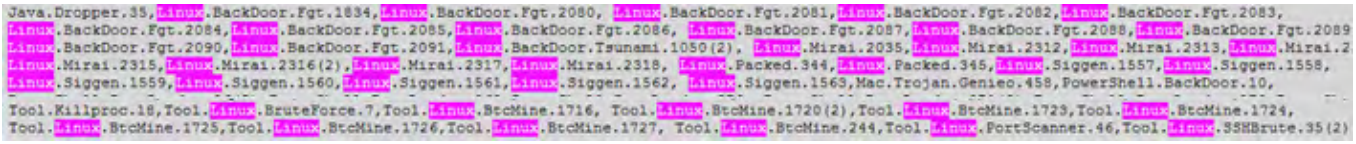
> Вирусов под Linux не существует.
>
> *Февраль 2017*
> Источник

Многие «умные» (и не очень) устройства используют разновидности операционной системы Linux. При этом рядовые пользователи не утруждают себя сменой паролей и обновлением прошивок, а число тех же роутеров исчисляется миллионами.

Linux.LuaBot представляет собой набор из 31 Lua-сценария и двух дополнительных модулей, каждый из которых выполняет собственную функцию. Троянец способен заражать устройства **с архитектурами Intel x86 (и Intel x86_64), MIPS, MIPSEL, Power PC, ARM, SPARC, SH4, M68k** – иными словами, не только компьютеры, но и широчайший ассортимент роутеров, телевизионных приставок, сетевых хранилищ, IP-камер и других «умных» устройств.

Источник

Атаки на Linux стали трендом, что, в свою очередь, увеличило число хакеров, охотящихся за уязвимостями Linux-систем.

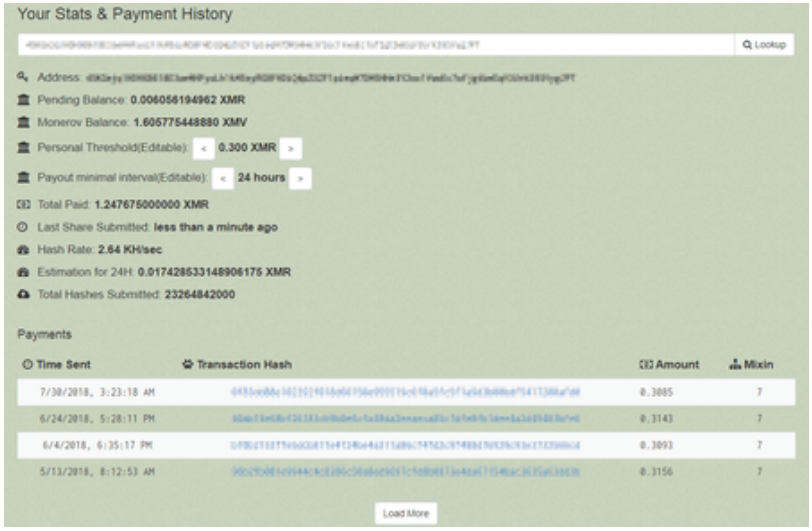


Источник

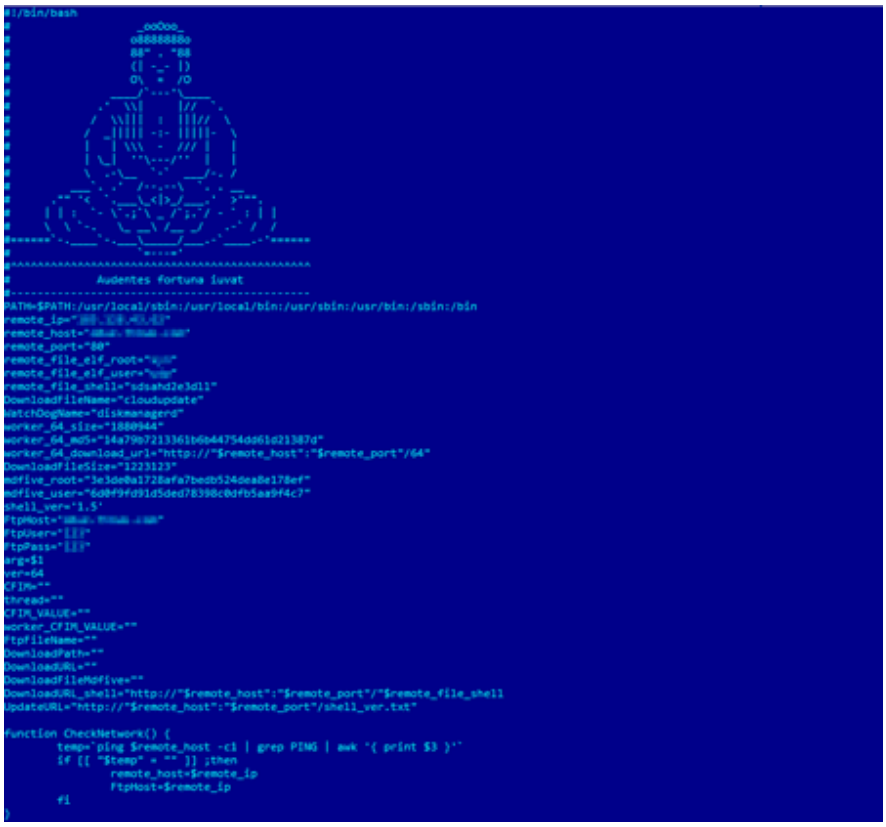
Tool.Linux.BruteForce...
Tool.Linux.PortScanner...
Tool.Linux.SSHBrute...
Tool.Linux.BtcMine...
В общем-то, обычный день. Отмеченный, разве что, малой активностью вирусописателей.

Приведенный выше скриншот говорит о том, для чего предназначены вредоносные программы, созданные под Linux. В основном это подбор паролей, поиск открытых портов для дальнейшей атаки и, конечно, майнинг.

Первые попытки заражения майнерами работающих под управлением Linux серверы были зафиксированы «Доктор Веб» в начале мая 2018 года. Киберпреступники соединялись с сервером по протоколу SSH, подбирали логин и пароль методом их перебора по словарю (bruteforce) и после успешной авторизации на сервере отключали утилиту iptables, управляющую работой межсетевого экрана. Затем злоумышленники загружали на атакованный сервер утилиту-майнер и файл конфигурации для нее. Чуть позже они начали использовать для этих целей вредоносные программы. Так, в августе вирусные аналитики обнаружили троянца Linux.BtcMine.82, написанного на языке Go. Он представлял собой дроппер, который устанавливал на зараженное устройство содержащийся в нем майнер.



В ноябре был описан Linux.BtcMine.174. Он представляет собой большой сценарий, написанный на языке командной оболочки sh и содержащий более 1000 строк кода. Троянец состоит из нескольких модулей и умеет заражать другие устройства в сети. Кроме того, он скачивает и устанавливает на инфицированной машине одну из версий троянца Linux.BackDoor.Gates.9, предназначенного для выполнения поступающих от злоумышленников команд и осуществления DDoS-атак.



Установившись в системе, Linux.BtcMine.174 ищет конкурирующие майнеры и при обнаружении завершает их процессы. Если Linux.BtcMine.174 не был запущен от имени суперпользователя (root), для повышения своих привилегий в зараженной системе он использует **набор эксплойтов**. Вирусные аналитики «Доктор Веб» выявили как минимум два применяемых Linux.BtcMine.174 эксплойта: это Linux.Exploit.CVE-2016-5195 (также известный под именем DirtyCow) и Linux.Exploit.CVE-2013-2094, при этом загруженные из Интернета исходники DirtyCow троянец **компилирует прямо на зараженной машине**.

Linux.BtcMine.174 скачивает и запускает на инфицированном устройстве руткит – также в виде сценария sh, основанном на исходном коде, который ранее был опубликован в свободном доступе. Среди функций руткит-модуля можно выделить кражу вводимых пользователем паролей команды su, сокрытие файлов в файловой системе, сетевых соединений и запускаемых процессов. Троянец собирает информацию о сетевых узлах, к которым ранее подключались по протоколу ssh, и пробует заразить их.

Источник

На данный момент для ОС Linux создано более 1700 вредоносных майнеров

Но возможности вредоносных программ бывают и шире.

Среди вредоносных программ, разработанных для этих ОС, необходимо отметить Linux.Hanthie. Этот бот имеет механизм антиобнаружения, характеризуется возможностью скрытой автозагрузки, не требующей привилегий администратора, использует стойкое шифрование для взаимодействия с панелью управления и обладает возможностью гибкой настройки через файл конфигурации. После запуска троянец блокирует доступ к адресам, с которых осуществляется установка обновлений или загрузка анти-

вирусного ПО. В троянце предусмотрены средства противодействия анализу и запуску в изолированных и виртуальных окружениях. Троянец может работать в различных дистрибутивах Linux, в том числе Ubuntu, Fedora и Debian, и поддерживает восемь типов десктоп-окружений, например, GNOME и KDE. Основной вредоносный функционал Linux.Hanthie заключается в перехвате и отправке злоумышленникам содержимого заполняемых пользователем форм. Кроме того, троянец реализует функции бэкдора. Троянец Linux.Sshdkit предназначен для похищения логинов и паролей. Существуют разновидности Linux.Sshdkit и для 32-разрядных, и для 64-разрядных версий дистрибутивов Linux. После успешной установки в систему троянец встраивается в процесс sshd, перехватывая функции аутентификации. После установки сессии и успешного ввода пользователем логина и пароля те отправляются на принадлежащий злоумышленникам удаленный сервер. Только за май 2013 года троянец передал на перехваченный аналитиками «Доктор Веб» управляющий узел данные для доступа к 562 инфицированным Linux-серверам, среди которых в том числе встречаются серверы крупных хостинг-провайдеров.

Зачастую разрабатываемое злоумышленниками ПО может быть универсальным – так, одна из критических уязвимостей Java позволила организовать атаки на компьютеры, работающие под управлением macOS, Linux и Windows, а уязвимость в Adobe Flash Player позволила атаковать Windows, macOS, Linux, Solaris и некоторые версии Android при помощи специально оформленного swf-файла.

> Turla использовался для кибер-шпионажа в 45 странах. И находили его, как правило, в правительственных организациях, посольствах и муниципальных учреждениях.
> Спецслужбы?

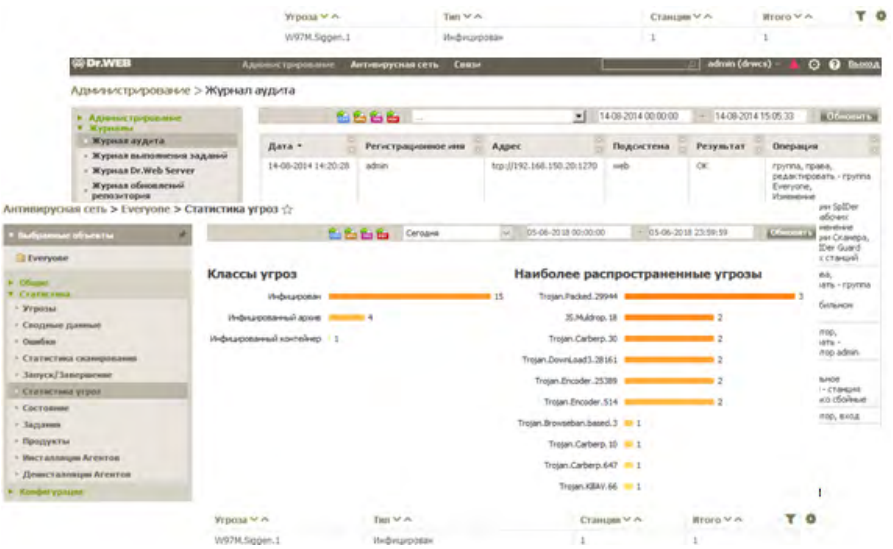
Как вредоносные программы проникают на Linux?

В большинстве случаев вредоносные программы попадают на Linux из-за невнимательности пользователей, когда те посещают вполне легитимные сайты (в том числе новостные) или загружают файлы из недоверенных источников. В этих случаях для установки вредоносной программы злоумышленникам не нужно взламывать компьютер. Взломав сайт, преступники могут заразить компьютеры его посетителей вне зависимости от установленной ОС – выбор системы при заражении зачастую осуществляется автоматически.

Однако проникновение может осуществляться и через уязвимости – так, например, действовал широко известный Linux.Sshdkit. В связи с этим необходимо отметить, что пренебрежение обновлениями как самой операционной системы, так и установленных на ней приложений, использование крайне слабых паролей (а то и вообще паролей по умолчанию) – прямой путь к передаче компьютеров в руки злоумышленников. Еще один вариант – вредоносные программы, работающие непосредственно на сайте. Например, майнеры, реализованные в виде JavaScript.

Чем можно защитить операционные системы UNIX и работающие на них сервисы?

Компания «Доктор Веб» предлагает решения для защиты рабочих станций, файловых серверов, почтовых серверов и шлюзов. Все они могут управляться в том числе и централизованно.



Центр управления – это простота установки и гибкость настроек, автоматизированное и легко контролируемое развертывание Dr.Web, возможности гибкого конфигурирования через консоль администратора. Администратор сети может управлять защитой с помощью веб-интерфейса, утилит командной строки, контролировать работу защиты из внешних систем.

Решение для защиты рабочих станций, а также личных компьютеров Dr.Web для Linux – это:

- Ограничение доступа к потенциально опасным интернет-ресурсам с помощью тематических баз, а также черных и белых списков.
- Блокировка отправки и приема электронной почты, содержащей вредоносные объекты или нежелательные ссылки.
- Мониторинг сетевых соединений и полная проверка веб-трафика, в том числе защищенных соединений.
- Защита от угроз для ОС Windows, запускаемых под ОС Linux, в том числе с помощью Облака Dr.Web.
- Возможность защиты рабочих станций даже тех сотрудников, которые находятся в командировке или отпуске — т. е. при отсутствии доступа к Центру управления антивирусной защитой.

Решение для защиты почтовых серверов **Dr.Web для почтовых серверов UNIX** – это:

- Чистый трафик от ваших партнеров и клиентов. Взлом домена или перехват трафика злоумышленниками не даст им возможности послать вам вирус или спам.
- Блокировка отправки и приема электронной почты, содержащей вредоносные объекты или нежелательные ссылки.
- Защита от фишинга.
- Безопасная работа сотрудников дома и в командировках.
- Высокая производительность и стабильность работы. Dr.Web работает не только на отдельно стоящих серверах, но и на кластерах. В случае кластерного решения лицензировать необходимо только одну копию, что существенно снижает затраты на антивирусную защиту.
- Поддержка систем мониторинга. Dr.Web для почтовых серверов UNIX может быть интегрирован любыми системами мониторинга – от локально расположенных в сети компании и до систем центров ГосСОПКА.
- Распределенная проверка. Защищаемые данные могут передаваться на проверку на удаленные серверы или различные узлы кластерных систем.
- Локальное облако. Возможности Dr.Web для UNIX позволяют компонентам решения обмениваться обновлениями, результатами проверки файлов, передавать друг другу на проверку файлы, а также предоставлять услуги сканирующего ядра.

- Защита объектов операционной системы, на которой установлен Dr.Web для почтовых серверов UNIX Периодическая проверка сервера производится встроенным антивирусным сканером.
- Защита данных, загружаемых на сервер из сети и передаваемых с него во внешнюю сеть, на наличие угроз, и предотвращение соединения с узлами сети, внесенными как в категории нежелательных веб-ресурсов, так и в черные списки, формируемые системным администратором.
- Встроенный компонент Dr.Web Firewall для Linux. Защита сервера от взлома и возможность проверки почтового трафика без ограничений, накладываемых почтовым сервером.
- Возможность работы при 500 МБ свободной оперативной памяти.

! **Максимальное качество фильтрации** почтового трафика достигается в случае использования почтового шлюза **Dr.Web SMTP proxy** — фильтра, обрабатывающего сообщения до их попадания на почтовый сервер.

Dr.Web SMTP proxy:

- Существенно **повышает безопасность** сети в целом
- Защищает почтовый сервер компании от атак злоумышленников
- Значительно **улучшает качество фильтрации** за счет отсутствия ограничений, накладываемых почтовыми серверами
- **Снижает нагрузки** на внутренние почтовые серверы и рабочие станции
- **Повышает стабильность работы** системы проверки почты

Решение для защиты почтовых серверов **Dr.Web для интернет-шлюзов UNIX** – это:

- Полная проверка веб-трафика, в том числе защищенных соединений. Чистый трафик от ваших партнеров и клиентов. Взлом домена или перехват трафика злоумышленниками не даст им возможности послать вам вирус.
- Ограничение доступа к потенциально опасным интернет-ресурсам с помощью тематических баз, а также черных и белых списков.
- Непосредственная защита самого сервера от атак злоумышленников, включая периодическую проверку объектов файловой системы.
- Удаленная проверка систем, установка антивируса на которые невозможна.

- Поддержка систем мониторинга. Dr.Web для интернет-шлюзов UNIX может быть интегрирован с любыми системами мониторинга — от локально расположенных в сети компании и до систем центров ГосСОПКА.
- Распределенная проверка. Защищаемые данные могут передаваться на проверку на удаленные серверы или различные узлы кластерных систем.
- Минимальная совокупная стоимость. Dr.Web работает не только на отдельно стоящих серверах, но и на кластерах. В случае кластерного решения лицензировать необходимо только одну копию, что существенно снижает затраты на антивирусную защиту.
- Защита объектов операционной системы, на которой установлен Dr.Web для интернет-шлюзов UNIX. Периодическая проверка сервера производится встроенным антивирусным сканером.
- Локальное облако. Возможности Dr.Web для интернет-шлюзов UNIX позволяют компонентам решения обмениваться обновлениями, результатами проверки файлов, передавать друг другу на проверку файлы, а также предоставлять услуги сканирующего ядра.
- Возможность проверки удаленных устройств. Dr.Web для интернет-шлюзов UNIX позволяет выполнить удаленную проверку не только обычных компьютеров, но и устройств «Интернета вещей» — роутеров, ТВ-приставок.
- Ограничение данных, передаваемых через интернет-шлюз, а также ограничение доступа к шлюзу со стороны отдельных компьютеров.
- Встроенный компонент Dr.Web Firewall для Linux. Защита сервера от взлома.

Для перехода на другие решения или ОС смена или дозакупка лицензии не требуется!

С какими операционными системами UNIX совместимы решения Dr.Web?

Dr.Web совместим с любыми операционными системами Linux на основе ядра с версией 2.6.37 и выше, использующие glibc 2.13 и выше. В частности AstraLinux 1.3 – 1.6 Special Edition «Смоленск»). Решения для почтовых серверов и шлюзов также совместимы с FreeBSD 10.3 и выше.

Исполняемые файлы Dr.Web подписаны цифровой подписью производителя ОС (АО «НПО РусБИТех»). Продукты могут работать во всех режимах AstraLinux, в том числе в мандатном режиме, с разными PARSEC уровнями привилегий.

Дистрибутивы, соответствующие описанным требованиям, по мере их выхода включаются в список поддерживаемых в формуляре – после соответствующей процедуры.

Подробные системные требования, а также варианты настроек для работы в различных средах, описаны в документации.

От чего защищают решения Dr.Web для Linux?

От всех видов вредоносных программ – в том числе созданных специально для ОС Linux.

Установка антивирусной защиты на UNIX-машины необходима не только для их защиты – она требуется для предотвращения заражения других ПК, работающих под управлением иных ОС и не имеющих эффективной защиты.

Кроме того, решения Dr.Web для Linux могут использоваться для защиты устройств и рабочих станций, не имеющих установленной антивирусной защиты.

Технологии защиты Dr.Web

Ежедневно на анализ в вирусную лабораторию «Доктор Веб» поступает до 12 миллионов программ. Такой огромный поток позволяет разбить поступающие данные на характерные участки и выделить среди них вредоносные. Технологии машинного обучения на основе полученных данных позволяют автоматически вырабатывать новые правила — без участия аналитиков и практически мгновенно.

- **Возможность проверки удаленных устройств**
  Dr.Web для Linux позволяет выполнить удаленную проверку не только обычных компьютеров, но и устройств «Интернета вещей» — роутеров, ТВ-приставок.
- **Высокая скорость сканирования и актуальность в любой момент времени**
  Компактные вирусные базы и технология несигнатурного поиска неизвестных вирусов Origins Tracing™ и развитый эвристический анализ позволяют обнаружить любые, даже неизвестные в момент атаки вредоносные программы.
- **Защита от ранее неизвестных вредоносных программ**
  Все защищаемые файлы и документы проверяются в момент обращения к ним с использованием технологии обнаружения неизвестных вредоносных объектов новейших типов, в том числе скрытых неизвестными упаковщиками.

Несигнатурные методы детектирования неизвестных угроз Dr.Web Enterprise Security Suite – это:

- Возможность обнаружения угроз без постоянного обращения к вирусным базам – что положительно сказывается как на быстродействии, так и качестве обнаружения новейших угроз
- Обнаружение угроз до фактического исполнения их кода
- Обнаружение популярных в данных момент действий злоумышленников: использование вредоносных майнеров, загрузчиков вредоносного ПО – как активных, так и предназначенных к запуску во всех областях системы.

Для дома	Для бизнеса
90 дней	30 дней
https://download.drweb.ru/linux/	https://download.drweb.ru/demoreq/biz/v2 При необходимости использования сертифицированной версии укажите тип сертификации.

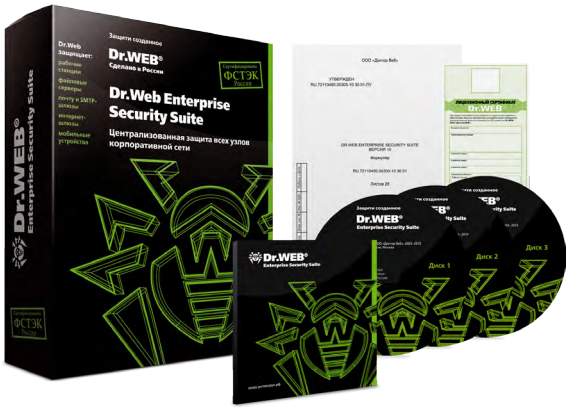
Лицензии и сертификаты

Согласно действующему законодательству, государственные органы, а также компании и организации, защищающие:

- данные в системах, в которых обрабатываются сведения, составляющие государственную тайну;
- персональные и конфиденциальные данные;
- критически-важную инфраструктуру,
- обязаны использовать сертифицированные антивирусные решения.
- «Доктор Веб» имеет сертификаты ФСТЭК России и Минобороны России (ИТ.САВЗ.А2.ПЗ, ИТ.САВЗ.Б2.ПЗ, ИТ.САВЗ.В2.ПЗ, ИТ.САВЗ.Г2.ПЗ), ФСБ России (классов А2, Б2, В2, Г2, Д2 для защиты гостайны).

- Использование антивирусов Dr.Web обеспечивает выполнение требований норм регуляторов по защите ИСПДн до 1 уровня защищенности включительно, ГИС до 1 класса защищенности включительно, систем обработки сведений, содержащих гостайну, объектов КИИ вплоть до высшей категории.
- Наличие у «Доктор Веб» сертификатов свидетельствует об отсутствие недекларированных возможностей и полном соответствии нормативным правовым актам регуляторов в части создания и сертификации средств защиты информации.
- «Доктор Веб» имеет лицензию ФСБ на проведение работ, связанных с государственной тайной.

Сертифицированный медиапакет Dr.Web

	Комплектация
	▪ Коробка Dr.Web для бизнеса сертифицированный ▪ Лицензионный сертификат с серийным номером ко всем продуктам Dr.Web, указанным на коробке. ▪ 3 DVD-диска в фирменных конвертах, содержащие верифицированные дистрибутивы сертифицированных продуктов Dr.Web Enterprise Security Suite версии 11, а также документацию и материалы в формате PDF для настройки поставляемого программного обеспечения в соответствии с сертифицированными параметрами, приведенными в технической документации. ▪ Формуляр с голографической наклейкой, в котором содержатся эталонные значения контрольных сумм сертифицированных ФСТЭК России продуктов Dr.Web Enterprise Security Suite версии 11.

С сертифицированными ФСТЭК России медиапакетами можно купить следующие лицензии Dr.Web:

Dr.Web Dr.Web Enterprise Security Suite	**Комплект Dr.Web Универсальный**	**Dr.Web «Малый бизнес»**	**Комплект Dr.Web для школ**
Любое ко-во ПК ПК	От 5 ПК + 1 сервер	5 ПК + 1 сервер	От 10 ПК + 1 сервер

Что такое сертифицированное ПО?

- ПО, прошедшее проверку соответствия в Системе сертификации средств защиты информации в соответствии с требованиями государственных стандартов и нормативных документов по защите информации, что подтверждается Сертификатом соответствия.

Dr.Web Enterprise Security Suite сертифицирован в соответствии с требованиями федеральных органов сертификации ФСТЭК России и ФСБ России и внесен в «Единый реестр российских программ для электронных вычислительных машин и баз данных» Министерства связи и массовых коммуникаций РФ.
В связи с наличием сертификатов соответствия требованиям к средствам антивирусной защиты (Приказ ФСТЭК России от 20.03.2012 г. № 28), а также в соответствии с положениями:

- Федерального закона № 152-ФЗ «О персональных данных»;
- Профилей защиты средств антивирусной защиты типа «А», «Б», «В» и «Г» второго класса защиты;
- Руководящего документа Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»;

только **Dr.Web Enterprise Security Suite** может быть использован для обеспечения 1-го уровня защищенности персональных данных, ГИС вплоть до 1-го класса защищенности включительно, защиты объектов критической инфраструктуры вплоть до высшего уровня, объектов Минобороны РФ, а также организаций, работающих с МО РФ, систем, содержащих документы с уровнем «Совершенно секретно».

- ПО, дистрибутив которого соответствует эталонному экземпляру, подвергавшемуся сертификационным испытаниям, что подтверждается соответствующими записями в сопроводительной документации на сертифицированное ПО (формуляре), и специальным голографическим знаком соответствия с уникальным номером, который идентифицирует данный экземпляр в системе государственного учета сертифицированных продуктов.
- ПО, установленное и настроенное в соответствие с сертифицированными параметрами.
- ПО, все доработки (обновления) которого, критичные для безопасности, также подвергаются сертификационным испытаниям.
- ПО, на которое имеется возможность получения официального подтверждения подлинности продукта в госорганах.

Кому необходимо использовать версии, сертифицированные ФСБ России?

Продукты, сертифицированные ФСБ России, необходимо использовать, если

- используется удостоверяющий центр;
- есть криптозащита и шифрование;
- есть требования от ФСБ России использовать сертифицированный антивирус.

Если таких требований нет, то можно использовать Dr.Web, сертифицированный ФСТЭК России.

Как получить дистрибутив и установить антивирус?

Дистрибутив антивируса может поставляться в двух вариантах: в виде универсального пакета для UNIX-систем (run-пакета) и в виде пакетов для конкретных операционных систем (например, rpm- или deb-пакетов).

Если необходима сертифицированная версия, то в связи с тем, что по действующим правилам запрещено размещать дистрибутивы в общем доступе, установка может быть проведена с DVD-диска. В случае срочной необходимости клиент может обратиться в службу поддержки и запросить ссылки для скачивания сертифицированных версий и формуляра. К запросу надо приложить документы об оплате сертифицированного медиапакета.

Переустанавливать Dr.Web после получения медиапакета с DVD не нужно.

Формуляр следует распечатать, в разделе «Особые отметки» необходимо сделать пометки о замене формуляра RU.72110450.00300-10 30 02 с голографической наклейкой (знаком соответствия системы сертификации) на обновленный формуляр RU.72110450.00300-10 30 02 изм.4.

В случае однопользовательской версии Антивируса Dr.Web для Linux установка и обновление могут быть осуществлены с помощью как графического, так и интерактивного консольного инсталлятора. Для установки необходимы права администратора системы.

Как обновить сертифицированную версию?

В случае срочной необходимости клиент может обратиться в службу поддержки и запросить ссылки для скачивания сертифицированных версий и формуляра. К запросу надо приложить документы об оплате сертифицированного медиапакета.

На замененном формуляре RU.72110450.00300-10 30 02 можно добавить: «Формуляр аннулирован. Знак соответствия системы сертификации (голографическая наклейка) действителен». Замененный формуляр следует хранить вместе с обновленным для сохранения знака соответствия системы сертификации.

Как получить обновления для замкнутой сети?

Для обновления вирусных баз отдельной станции необходимо использовать сертифицированный антивирус для рабочей станции и иметь возможность синхронизировать полученные базы. Также можно использовать штатную утилиту drwreploader.

Для обновления централизованно управляемой сети необходимо использовать утилиту обновления из состава Dr.Web Enterprise Security Suite.

Предпродажная поддержка	Техническая поддержка
▪ Бесплатное тестирование продуктов Dr.Web — в сети заказчика или удаленно в виртуальной среде ▪ Развертывание, помощь при внедрении (по телефону или с выездом на территорию заказчика (только в Москве) ▪ Презентация, вебинар, семинар ▪ Помощь в написании или проверке уже написанного технического задания.	▪ Круглосуточно — по телефону и через форму https://support.drweb.ru ▪ В России, на русском языке ▪ Бесплатные услуги поддержки и бесплатная расшифровка от троянцев-вымогателей для лицензий в прайсовом диапазоне (до 250 адресов почты) ▪ Стоимость поддержки для запрайсовых и безлимитных лицензий оговаривается особо ▪ Платная VIP-поддержка.

Экспертиза вирусозависимых компьютерных инцидентов (ВКИ)

Если ваша компания пострадала от действий вредоносного ПО и требуется квалифицированная экспертиза вирусных аналитиков, воспользуйтесь услугами специального подразделения компании «Доктор Веб».

Об экспертизе ВКИ

Заявки на экспертизу

«Доктор Веб» — российский производитель антивирусных средств защиты информации под маркой Dr.Web. Продукты Dr.Web разрабатываются с 1992 года.

125040, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп. 12а
Тел.: +7 495 789-45-87 (многоканальный), факс: +7 495 789-45-97

https://антивирус.рф • https://www.drweb.ru • https://free.drweb.ru • https://curenet.drweb.ru