Dr.WEB®
с 1992 года

Риски и угрозы в Интернете вещей (IoT)

Введение

Сейчас во Всемирную сеть выходят не только компьютеры, смартфоны, планшеты и роутеры, но также смарт-телевизоры, камеры видеонаблюдения, «умные» часы, холодильники, автомобили, фитнес-трекеры, видеорегистраторы и даже детские игрушки. Количество устройств Интернета вещей уже превышает несколько миллиардов, и с каждым годом их число растет.

Многие из них плохо или совсем не защищены от атак. Например, для подключения к ним могут использоваться простые или общеизвестные пары «логин — пароль», которые по умолчанию устанавливаются на сотни тысяч моделей. Их владельцы либо не задумываются об изменении заданных на заводе настроек, либо не могут этого сделать из-за ограничений самих производителей. Злоумышленники относительно легко получают доступ к таким устройствам, используя подбор комбинаций по словарю (так называемый *brute force* — метод грубой силы). Кроме того, они могут эксплуатировать уязвимости установленных на них операционных систем.

С 2016 года компания «Доктор Веб» пристально следит за угрозами сегмента Интернета вещей. Для этого наши специалисты развернули сеть специализированных приманок — ханипотов (от слова honeypot — горшочек с медом). Такие ловушки имитируют различные типы «умных» электронных устройств и регистрируют попытки их заражения. Ханипоты охватывают сразу несколько аппаратных платформ, в числе которых ARM, MIPS, MIPSEL, PowerPC и Intel x86_64. Они позволяют отслеживать векторы атак, обнаруживать и исследовать новые образцы вредоносных программ, улучшать механизмы их обнаружения и более эффективно бороться с ними.

В этом материале представлены сведения о выявленных атаках на «умные» устройства, а также о наиболее распространенных угрозах для Интернета вещей.

Статистика

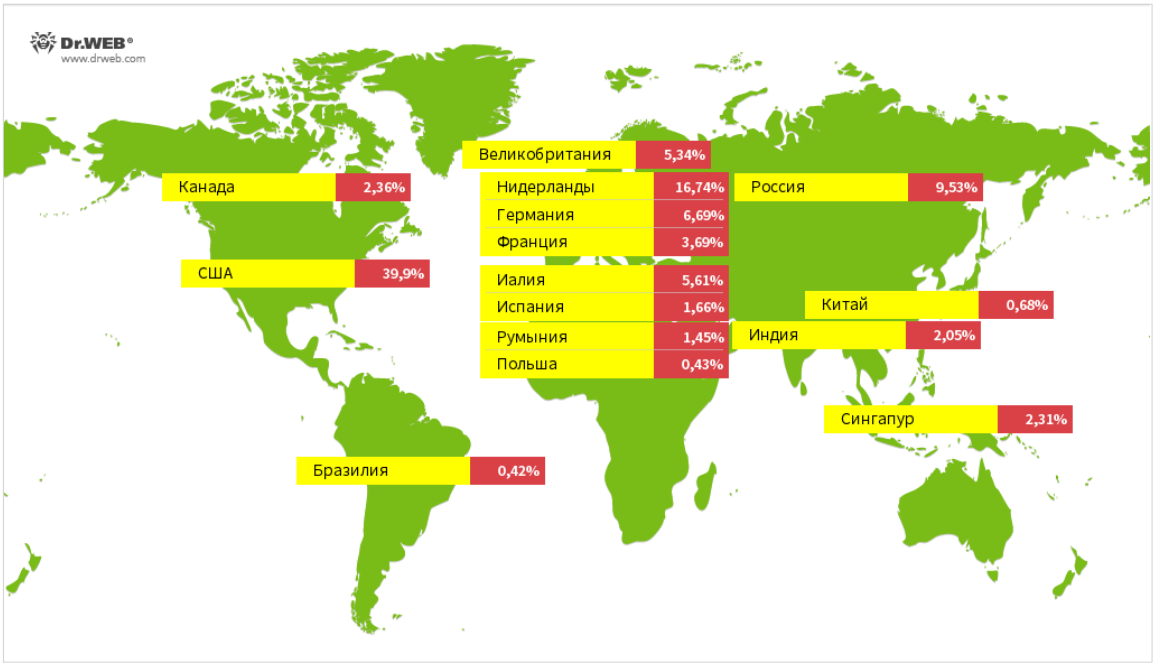
В самом начале наблюдения вирусные аналитики фиксировали относительно низкую активность вредоносных программ, нацеленных на устройства Интернета вещей. За четыре месяца 2016 года специалисты «Доктор Веб» выявили 729 590 атак, однако всего через год — в 32 раза больше, 23 741 581. Еще через 12 месяцев их было уже 99 199 434. Что же касается текущего года, то лишь за первые шесть месяцев было совершено 73 513 303 атаки — почти столько же, сколько за весь 2018 год.

Динамика обнаружения ханипотами атак показана на графике:

Менее чем за три года количество попыток взлома и заражения устройств Интернета вещей возросло на 13 497%.

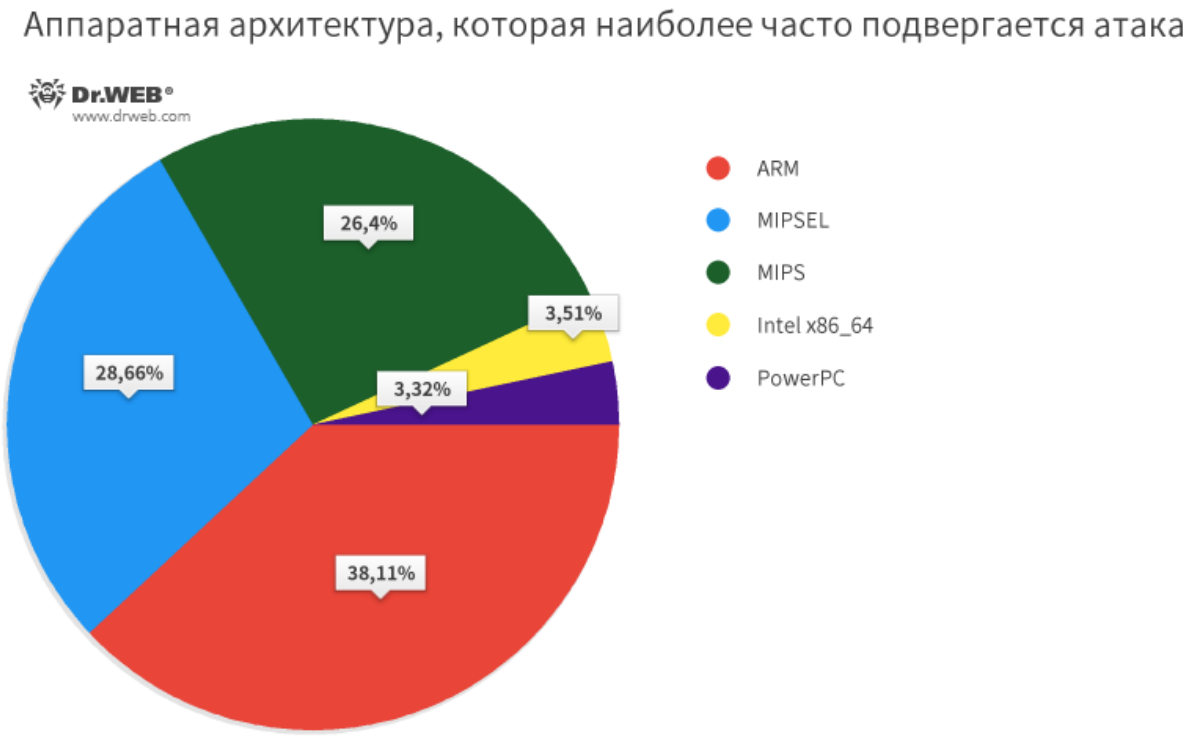
Атаки на «умные» устройства выполнялись с IP-адресов, расположенных в более чем 50 странах. Чаще всего это были США, Нидерланды, Россия, Германия, Италия, Великобритания, Франция, Канада, Сингапур, Индия, Испания, Румыния, Китай, Польша и Бразилия.

Географическое распределение источников атак и их процентное соотношение показано на следующем графике:



После успешной компрометации устройств злоумышленники могут загружать на них одного или нескольких троянцев. В общей сложности число уникальных вредоносных файлов, обнаруженных нашими ловушками за время наблюдения, составило 131 412. Динамика их выявления показана ниже.

«Умные» устройства работают на различных процессорных архитектурах, и у многих вредоносных программ есть версии сразу для нескольких аппаратных платформ. Среди тех из них, которые имитируют наши ханипоты, чаще всего атакам подвергаются устройства с процессорами ARM, MIPSEL и MIPS. Это хорошо видно на диаграмме:



Согласно полученной ханипотами статистике, самые активные вредоносные программы — представители семейства Linux.Mirai, на которых приходится более 34% атак. За ними следуют загрузчики Linux.DownLoader (3% атак) и троянцы Linux.ProxyM (1,5% атак).

В первую десятку также входят вредоносные приложения Linux.Hajime, Linux.BackDoor.Fgt, Linux.PNScan, Linux.BackDoor.Tsunami и Linux.HideNSeek. Процентное соотношение наиболее активных троянцев представлено на следующей иллюстрации:

Вредоносные программы, которые атакуют «умные» устройства, условно можно разделить на несколько базовых категорий в соответствии с их основными функциями:

- трояны для проведения DDoS-атак (пример: Linux.Mirai);
- трояны, которые распространяют, загружают и устанавливают другие вредоносные приложения и вспомогательные компоненты (пример: Linux.DownLoader, Linux.Mul-Drop);
- трояны, позволяющие удаленно управлять зараженными устройствами (пример: Linux.BackDoor);
- трояны, превращающие устройства в прокси-серверы (пример: Linux.ProxyM, Linux.Ellipsis.1, Linux.LuaBot);
- трояны для майнинга криптовалют (пример: Linux.BtcMine);
- другие.

Однако большинство современных вредоносных программ представляют собой многофункциональные угрозы, поскольку многие из них могут сочетать в себе сразу несколько функций.

Тенденции в сфере угроз для «умных» устройств

- Из-за доступности исходных кодов троянцев, таких как Linux.Mirai, Linux.BackDoor.Fgt, Linux.BackDoor.Tsunami и др., растет количество новых вредоносных программ.

- Появление все большего числа вредоносных приложений, написанных на «нестандартных» языках программирования, например Go и Rust.
- Злоумышленникам доступна информация о множестве уязвимостей, эксплуатация которых помогает заражать «умные» устройства.
- Сохраняется популярность майнеров, добывающих криптовалюты (преимущественно Monero) на устройствах Интернета вещей.

Ниже представлена информация о наиболее распространенных и примечательных троянцах для Интернета вещей.

Подробнее об угрозах для Интернета вещей

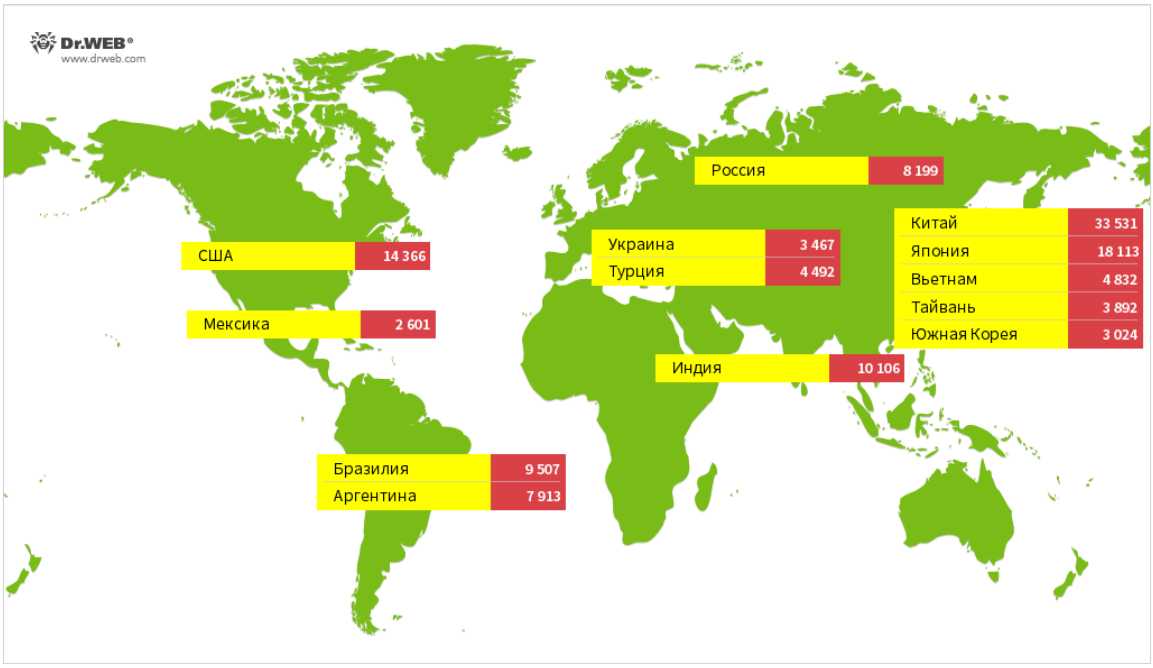
Linux.Mirai

Linux.Mirai — один из наиболее активных троянцев, атакующих устройства Интернета вещей. Первая версия этого вредоносного приложения появилась в мае 2016 года. Позднее его исходные коды были опубликованы в свободном доступе, поэтому у него быстро появилось большое число модификаций, созданных различными вирусописателями. Сейчас Linux.Mirai — самый распространенный троянец для ОС Linux, который работает на множестве процессорных архитектур, таких как x86, ARM, MIPS, SPARC, SH-4, M68K и др.

После заражения целевого устройства Linux.Mirai соединяется с управляющим сервером и ждет от него дальнейших команд. Основная функция этого троянца — проведение DDoS-атак.

На следующем графике показана динамика обнаружения ханипотами активных копий этого вредоносного приложения:

Различные модификации Linux.Mirai наиболее активны в Китае, Японии, США, Индии и Бразилии. Ниже представлены страны, где за время наблюдений было зафиксировано максимальное число ботов этого семейства.

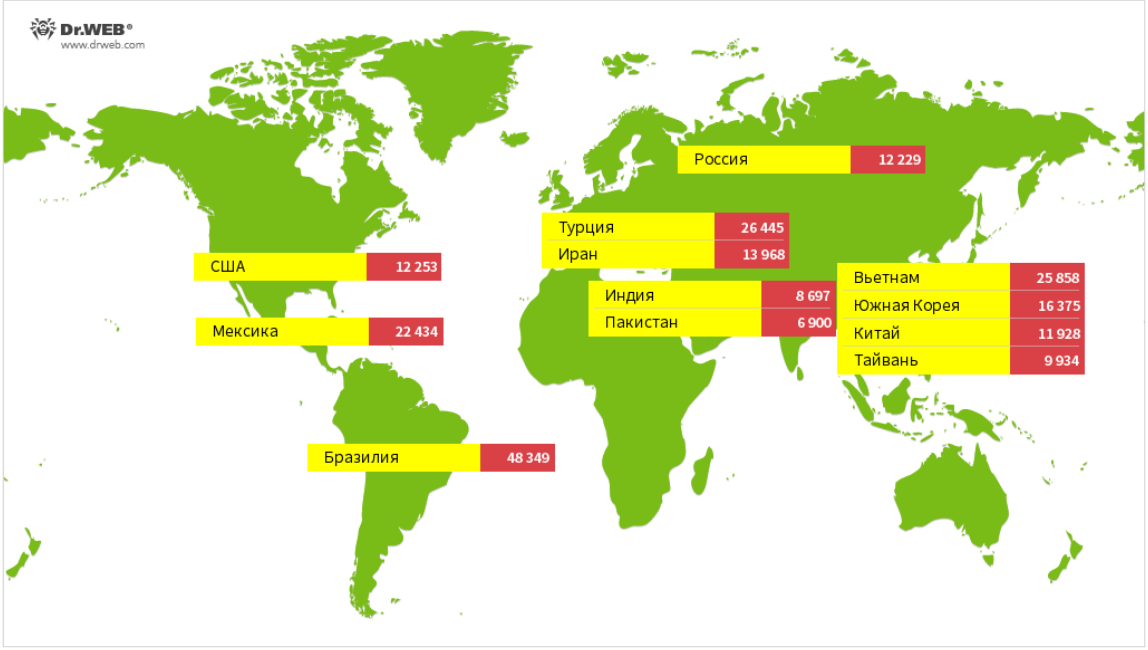


Linux.Hajime

Еще одним опасным вредоносным приложением, заражающим «умные» устройства, является Linux.Hajime. Этот троянец известен вирусным аналитикам с конца 2016 года. Он работает на архитектурах ARM, MIPS и MIPSEL и реализует функцию сетевого червя, распространяясь с использованием протокола Telnet. Инфицированные устройства включаются в децентрализованный P2P-ботнет и используются для дальнейшего заражения доступных объектов в Сети. Вредоносная программа блокирует доступ других вредоносных программ к успешно атакованным устройствам, закрывая на них порты 23, 7547, 5555 и 5358.

Пик активности Linux.Hajime пришелся на конец 2016 — начало 2017 года, когда максимальное число одновременно активных копий троянцев этого семейства превышало 43 000. После этого активность вредоносных программ упала и продолжает постепенно снижаться. Сейчас число действующих ботов Linux.Hajime не превышает нескольких сотен.

Наибольшее распространение эти троянцы получили в Бразилии, Турции, Вьетнаме, Мексике и Южной Корее. На карте показаны страны с максимальным числом активных троянцев Linux.Hajime, которые были зафиксированы за всё время наблюдений.



Linux.BackDoor.Fgt

В пятерку троянцев, предназначенных для заражения устройств Интернета вещей, входит Linux.BackDoor.Fgt, который распространяется с осени 2015 года. Различные версии этого вредоносного приложения поддерживают работу на архитектурах MIPS, SPARC и др. и работают в среде ОС Linux. Исходный код Linux.BackDoor.Fgt находится в открытом доступе, поэтому он так популярен среди вирусописателей.

Эти бэкдоры распространяются с использованием протоколов Telnet и SSH, подбирая логины и пароли для доступа к атакуемым объектам. Основное предназначение этих троянцев — проведение DDoS-атак и дистанционный контроль зараженных устройств.

Linux.ProxyM

Троянец Linux.ProxyM — одна из вредоносных программ, которые злоумышленники используют для обеспечения собственной анонимности в Интернете. Она запускает на заражаемых Linux-устройствах SOCKS-прокси-сервер, через который киберпреступники пропускают сетевой трафик. Специалисты «Доктор Веб» обнаружили первые версии Linux.ProxyM в феврале 2017 года, и этот троянец по-прежнему активен.

Linux.Ellipsis.1

Linux.Ellipsis.1 — еще один троянец, предназначенный для превращения устройств Интернета вещей и компьютеров под управлением ОС Linux в прокси-серверы. Он попался аналитикам «Доктор Веб» в 2015 году. После запуска он удаляет файлы журналов и блокирует их повторное создание, удаляет некоторые системные утилиты, а также запрещает устройству устанавливать связь с определенными IP-адресами. Если троянец обнаруживает подозрительный трафик с одного из адресов, он также вносит этот IP в черный список. Кроме того, по команде управляющего сервера Linux.Ellipsis.1 прекращает работу приложений, которые подключались к запрещенным адресам.

Linux.LuaBot

Компания «Доктор Веб» обнаружила первые версии троянцев семейства Linux.LuaBot в 2016 году. Эти вредоносные приложения написаны на скриптовом языке Lua и поддерживают устройства с архитектурой Intel x86_64), MIPS, MIPSEL, Power PC, ARM, SPARC, SH4 и M68k. Они состоят из нескольких десятков скриптов-модулей, каждый их которых выполняет определенную задачу. Троянцы способны получать с управляющего сервера обновления этих модулей, а также загружать новые. Linux.LuaBot — многофункциональные вредоносные приложения. В зависимости от модификации вредоносных приложений и комплекта скриптов, злоумышленники могут использовать их для дистанционного управления зараженными устройствами, а также создания прокси-серверов для анонимизации в Сети.

Linux.BtcMine.174

Для злоумышленников майнинг (добыча) криптовалют — одна из основных причин заражения устройств Интернета вещей. В этом им помогают троянцы семейства Linux. BtcMine, а также другие вредоносные приложения. Одного из них — Linux.BtcMine.174 — специалисты «Доктор Веб» нашли в конце 2018 года. Он предназначен для добычи Monero (XMR). Linux.BtcMine.174 представляет собой скрипт, написанный на языке командной оболочки sh. Если он не был запущен от имени суперпользователя (root), троянец пытается повысить свои привилегии несколькими эксплойтами.

Linux.BtcMine.174 ищет процессы антивирусных программ и пытается завершить их, а также удалить файлы этих программ с устройства. Затем он скачивает и запускает несколько дополнительных компонентов, среди которых бэкдор и руткит-модуль, после чего запускает в системе программу-майнер.

Троянец прописывается в автозагрузку, поэтому ему не страшна перезагрузка инфицированного устройства. Кроме того, он периодически проверяет, активен ли процесс майнера. При необходимости он инициирует его вновь, обеспечивая непрерывность добычи криптовалюты.

Linux.MulDrop.14

Троянцы семейства Linux.MulDrop используются для распространения и установки других вредоносных приложений. Они работают на многих аппаратных архитектурах и типах устройств, однако в 2017 году вирусные аналитики «Доктор Веб» обнаружили троянца Linux.MulDrop.14, который целенаправленно атаковал компьютеры Raspberry Pi. Этот дроппер представляет собой скрипт, в теле которого хранится зашифрованная программа — майнер криптовалют. После запуска троянец распаковывает и запускает майнер, после чего пытается заразить другие устройства, доступные в сетевом окружении. Чтобы не допустить «конкурентов» к ресурсам зараженного устройства, Linux.MulDrop.14 блокирует сетевой порт 22.

Linux.HideNSeek

Вредоносная программа Linux.HideNSeek заражает «умные» устройства, компьютеры и серверы под управлением ОС Linux, объединяя их в децентрализованный ботнет. Для распространения этот троянец генерирует IP-адреса и пытается подключиться к ним, используя подбор логинов и паролей по словарю, а также список известных комбинаций аутентификационных данных. Кроме того, он способен эксплуатировать различные

уязвимости оборудования. Linux.HideNSeek может использоваться для удаленного управления зараженными устройствами — выполнять команды злоумышленников, копировать файлы и т. д.

Linux.BrickBot

В отличие от большинства других вредоносных программ, троянцы Linux.BrickBot не предназначены для получения какой-либо выгоды. Это вандалы, которые созданы для вывода из строя компьютеров и «умных» устройств, они известны с 2017 года.

Троянцы Linux.BrickBot пытаются заразить устройства через протокол Telnet, подбирая к ним логины и пароли. Затем они пытаются стереть данные с их модулей постоянной памяти, сбрасывают сетевые настройки, блокируют все соединения и выполняют перезагрузку. В результате для восстановления работы поврежденных объектов потребуется их перепрошивка или даже замена компонентов. Такие троянцы встречаются нечасто, но они крайне опасны.

В конце июня 2019 года получил распространение троянец Linux.BrickBot.37, также известный как Silex. Он действовал аналогично другим представителям семейства Linux.BirckBot — стирал данные с накопителей устройств, удалял их сетевые настройки и выполнял перезагрузку, после чего те уже не могли корректно включиться и работать. Наши ловушки зафиксировали свыше 2600 атак этого троянца.

Заключение

Миллионы высокотехнологичных устройств, которые всё больше используются в повседневной жизни, фактически являются маленькими компьютерами с присущими им недостатками. Они подвержены аналогичным атакам и уязвимостям, при этом из-за особенностей и ограничений конструкции защитить их может быть значительно сложнее или же вовсе невозможно. Кроме того, многие пользователи не до конца осознают потенциальные риски и всё еще воспринимают «умные» устройства как безопасные и удобные «игрушки».

Рынок Интернета вещей активно развивается и во многом повторяет ситуацию с началом массового распространения персональных компьютеров, когда механизмы борьбы с угрозами для них только обретали форму и совершенствовались. Пока производители оборудования и владельцы «умных» устройств адаптируются к новым реалиям, у злоумышленников есть огромные возможности для совершения атак. Поэтому в ближайшем будущем стоит ожидать появления новых вредоносных программ для Интернета вещей.

Компания «Доктор Веб» продолжает отслеживать ситуацию с распространением троянцев и других угроз для «умных» устройств и будет информировать наших пользователей обо всех интересных событиях в этой сфере. Антивирусные продукты Dr.Web успешно детектируют и удаляют названные в обзоре вредоносные программы.

О компании «Доктор Веб»

«Доктор Веб» — российский производитель антивирусных средств защиты информации под маркой Dr.Web. Продукты Dr.Web разрабатываются с 1992 года. Все права на технологии Dr.Web принадлежат компании «Доктор Веб». «Доктор Веб» — один из немногих антивирусных вендоров в мире, владеющих собственными уникальными технологиями детектирования и лечения вредоносных программ, имеет свою антивирусную лабораторию, глобальную службу вирусного мониторинга и службу технической поддержки, которые расположены в России.

Компания «Доктор Веб» — ключевой игрок на российском рынке программных средств обеспечения базовой потребности бизнеса — безопасности информации. Свой выбор в пользу продуктов Dr.Web сделали Государственная Дума Федерального Собрания РФ, ЦИК России, Минобороны России, Верховный Суд РФ, Совет Федерации Федерального Собрания РФ, Центральный банк Российской Федерации, многие другие государственные учреждения и крупнейшие компании.

Вот только некоторые клиенты Dr.Web: https://customers.drweb.com.

Dr.Web внесен в «Единый реестр российских программ для электронных вычислительных машин и баз данных» **Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации.**

Использование отечественного антивирусного ПО Dr.Web обеспечивает нашим клиентам защиту от рисков, связанных с изменением международной обстановки, таких как отказ в использовании, продлении, поставке или получении обновлений, а также от угроз, созданных для целенаправленных атак на предприятия и граждан России.

Со знаком качества

«Доктор Веб» имеет сертификаты, позволяющие использовать ПО Dr.Web в организациях с повышенными требованиями к уровню безопасности.

Dr.Web сертифицирован на отсутствие недекларированных возможностей – по 2 уровню контроля, на соответствие требованиям документа «Требования к средствам антивирусной защиты», утв. приказом ФСТЭК России № 28 от 20.03.2012 г., на соответствие требованиям ФСБ России к антивирусным средствам.

Продукты Dr.Web применяются для защиты информации, содержащейся в различных информационных системах, в том числе информации ограниченного доступа (государственная тайна, персональные данные и т. д.).

Использование ПО Dr.Web позволяет обеспечить надлежащее выполнение требований норм законодательства РФ о применении мер для защиты:

– информации с ограниченным доступом (государственная тайна, персональные данные и т. д.);
– отдельных категорий граждан от информации, причиняющей вред.

Сертификаты ФСТЭК России	**Сертификаты Минобороны России**	**Сертификаты ФСБ России**	**Все сертификаты и товарные знаки**

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://curenet.drweb.ru | https://free.drweb.ru