Dr.WEB®
с 1992 года

Dr.Web vxCube

- ОБЛАЧНЫЙ ИНТЕРАКТИВНЫЙ АНАЛИЗАТОР НЕИЗВЕСТНЫХ УГРОЗ (0-DAY), В ТОМ ЧИСЛЕ ИСПОЛЬЗУЕМЫХ ДЛЯ ЦЕЛЕВЫХ АТАК
- НЕМЕДЛЕННОЕ ИЗГОТОВЛЕНИЕ ЛЕЧАЩЕЙ УТИЛИТЫ ПО РЕЗУЛЬТАТАМ АНАЛИЗА
- ДЛЯ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И КИБЕРКРИМИНАЛИСТОВ

Dr.Web vxCube

Представьте, что, несмотря на защиту вашей сети антивирусом, вредоносный файл все-таки пробрался внутрь периметра. Или у вас появились обоснованные, на ваш взгляд, подозрения, что в сети завелся «чужой».

Правильной практикой будет отправить вызывающий сомнения файл на анализ в антивирусную лабораторию и дождаться вердикта. Но штучная работа аналитиков стоит дорого и требует подчас значительного времени.

А время не терпит: угрозу надо ликвидировать немедленно.

Незаменимым средством в таких ситуациях становится облачный интерактивный анализатор Dr.Web vxCube.

Dr.Web vxCube в течение **одной минуты** оценит вредоносность файла и изготовит лечащую утилиту для устранения последствий его работы.

▪ Не требует установки Работает в облаке	▪ Полный анализ поведения ВПО	▪ Понятные отчеты	▪ API для автоматизации работы с сервисом

Dr.Web vxCube — инновационное средство борьбы с новейшими неизвестными угрозами

Сегодня вирусописательство — это хорошо налаженный криминальный бизнес. Новые вредоносные программы, большинство из которых троянцы, появляются ежедневно сотнями тысяч. Не всё пришедшее на анализ в антивирусную лабораторию «Доктор Веб» — вредоносные программы. Но все они должны быть обработаны нашими специалистами. Анализ вредоносных файлов требует времени, также время уходит на сборку и тестирование обновлений, их выкладку на серверы обновлений, установку обновлений пользователями.

Задача антивируса — **не допускать заражения**.

При этом считается, что антивирус обязан обнаруживать все вредоносные программы в момент их проникновения. Однако технологически сложные и особо опасные троянцы, особенно созданные для извлечения коммерческой выгоды, вирусописатели проверяют на обнаружение по всем антивирусам, перед тем как выпустить свое творение в «живую природу», чтобы вирус существовал незамеченным антивирусами как можно дольше. Поэтому всегда существует временная дельта между выпуском троянца злоумышленниками, попаданием его образца на анализ в вирусную лабораторию и изготовлением противоядия.

Угроза заражения новейшим НЕИЗВЕСТНЫМ вирусом есть ВСЕГДА.

Проверить и убедиться, что файл вредоносен, выявить его обращения к локальным и сетевым ресурсам, а также получить специальную сборку лечащей утилиты Dr.Web CureIt! можно через сервис Dr.Web vxCube.

Что может натворить на вашем ПК троянец? Вы увидите это еще до того, как он начнет действовать.	**Каковы могут быть последствия гипотетической атаки на ваше предприятие?** Узнайте заранее.	**Что именно собирались делать злоумышленники в вашей сети?** Dr.Web vxCube разберет досконально.

Анализ производится в нескольких операционных системах, используются типичные приложения, которые сегодня больше всего атакуются злоумышленниками:

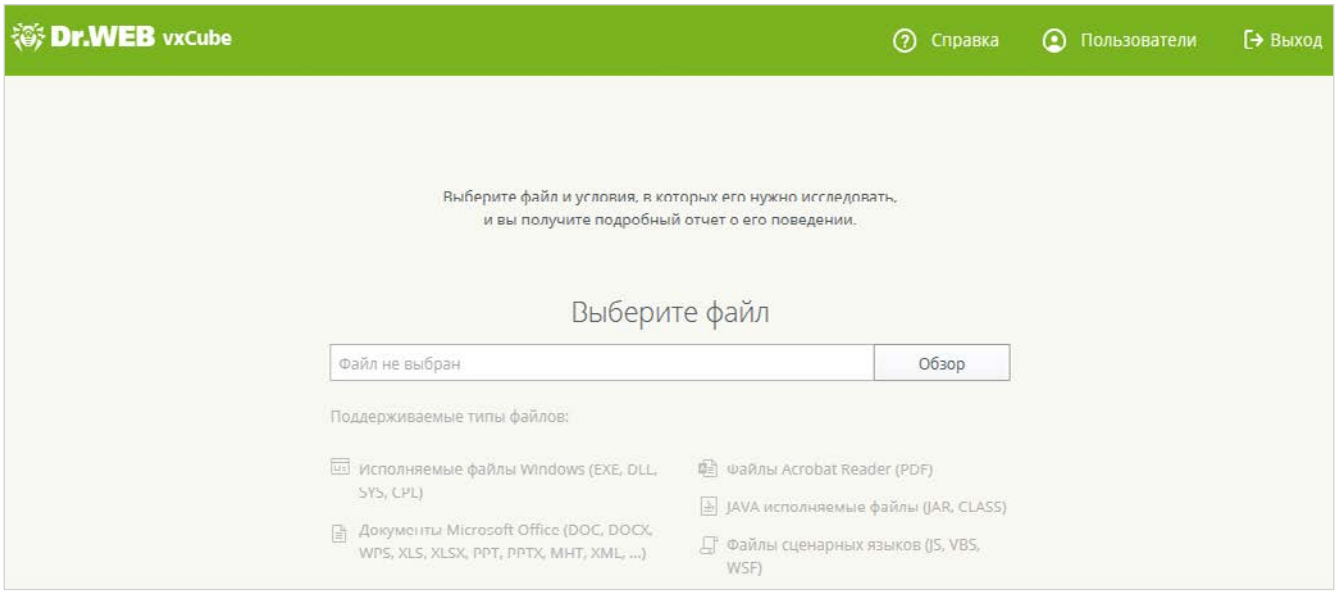
- Исполняемые файлы Windows
- Документы Microsoft Office
- Файлы Acrobat Reader
- Исполняемые файлы JAVA
- Скрипт-файлы

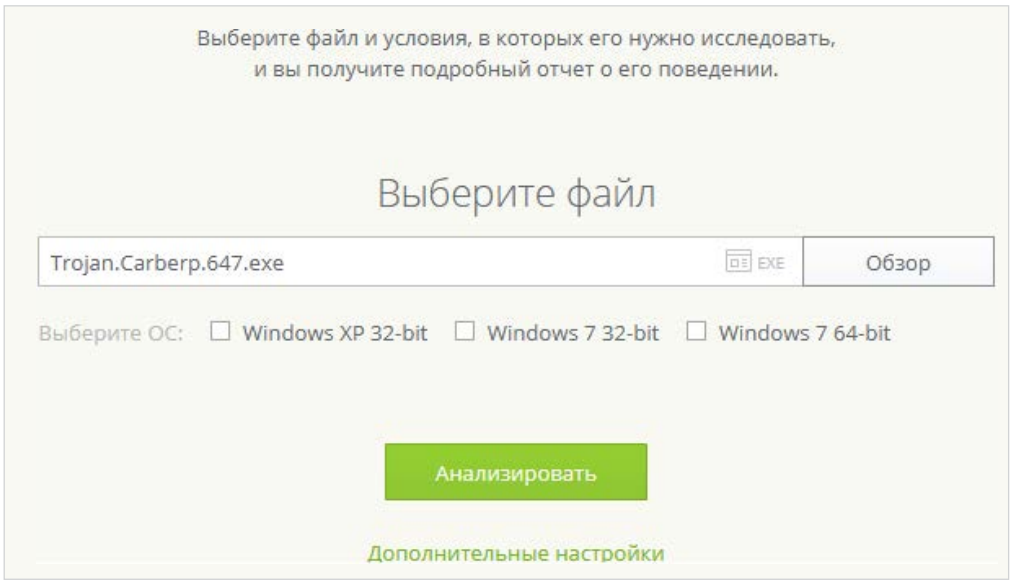
! Проверка подозрительного файла возможна как в ручном, так и в автоматическом режиме. Интеграция Dr.Web vxCube в сервисы компании позволяет не только увеличить количество проверяемых файлов, но и с высокой точностью выявлять новейшие, в том числе целевые атаки.

Как работает Dr.Web vxCube

1. Пользователь получает доступ к анализатору для отправки подозрительных файлов на «облачный» анализ.

Для входа в Dr.Web vxCube и работы в нем достаточно браузера и интернет-подключения.





Сервис бережно относится к персональным и конфиденциальным данным согласно принципам, прописанным в политике конфиденциальности «Доктор Веб»: https://company.drweb.ru/policy. Файлы, поступившие на анализ через Dr.Web vxCube, отделяются от файлов, поступивших иными путями.

2. **Анализатор запускает отправленный исследователем объект в изолированном окружении и изучает его поведение. Анализ производится автоматически, без участия вирусных аналитиков «Доктор Веб».**

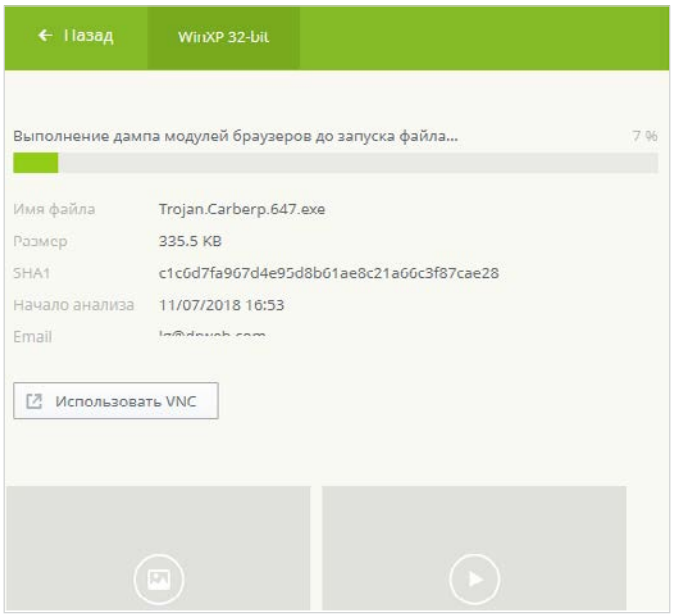
Проверка занимает от одной минуты!

Исследователь может:

- указать, в каких операционных системах и с какими версиями приложений должна происходить проверка;
- задать желаемое время проверки в настройках, если считает, что одной минуты недостаточно для полного анализа поведения подозрительного файла;

- удаленно — через интерфейс Dr.Web vxCube — наблюдать за ходом анализа и даже влиять на его ход, подключившись к анализатору через VNC (Virtual Network Computing) для участия в процессе исследования.

! Для управления процессом анализа в интерактивном режиме в браузере должно быть разрешено открытие всплывающих окон.



! Как известно, вредоносные программы отслеживают попытки своего запуска в специальном тестовом окружении и препятствуют своему анализу. В процессе разработки сервиса Dr.Web vxCube была создана виртуальная машина, защищенная от анализа вредоносными программами.

3. **Если объект однозначно представляет угрозу, пользователь немедленно получает специальную сборку лечащей утилиты Dr.Web CureIt!* для очищения системы от действий, произведенных проанализированным файлом.**

Это дает возможность максимально быстро обезвредить новейшую угрозу, не дожидаясь обновлений используемого антивируса.

Благодаря универсальности утилиты Dr.Web CureIt!, способной работать без установки в любой системе, где используется другой антивирус (не Dr.Web), это будет особенно полезно компаниям, пока не использующим Dr.Web в качестве основного средства защиты.

4. **По результатам анализа предоставляется отчет. Его можно просмотреть в личном кабинете пользователя Dr.Web vxCube или скачать в виде архива. Также в личном кабинете можно ознакомиться с результатами предыдущих проверок.**

! Отчет о результатах тестирования содержит данные об исследуемой программе, в частности участки ее кода, в связи с чем может детектироваться как вредоносная программа, при этом не представляя никакой опасности для компьютера.

* Если это входит в лицензию.

Отчеты сервиса Dr.Web vxCube

В итоговом отчете пользователю сервиса предоставляются следующие данные.

Оценка вредоносности

Сервис оценивает, является ли исследуемая программа вредоносной, а также насколько она может быть опасной.

Карта сетевой активности

Расскажет, к серверам в каких странах мира обращалась вредоносная программа.

Видеозапись

Продемонстрирует процесс запуска и работы файла.

Связи

Покажет, к каким файлам обращалась программа, в какие ветви реестра осуществлялась запись, какие интернет-ресурсы были использованы и т. д.

Техническая информация

Подскажет, что из системы нужно удалить, на защиту каких ее частей следует обратить повышенное внимание.

Созданные файлы

Приводится список файлов, создаваемых исследуемым образцом, и их контрольные суммы. Знание об этих файлах позволит удалить последствия заражения.

Журнал API

Покажет, как вредоносная программа прячется в системе.

! Согласно п. 6 Лицензионного соглашения для Dr.Web vxCube, публикация или иное распространение отчетов, в том числе с целью извлечения прибыли, должно быть письменно согласовано с «Доктор Веб».

Полезные ссылки

Демодоступ: https://download.drweb.ru/vxcube

Лицензирование: https://www.drweb.ru/vxcube/licensing

Анализ вредоносных файлов специалистами антивирусной лаборатории «Доктор Веб»

Ни один автоматизированный сервис никогда не заменит опыт и знания вирусного аналитика. В случае если вердикт Dr.Web vxCube о проанализированном файле будет не однозначно вредоносный, но у вас останутся сомнения в этом решении, предлагаем воспользоваться услугами специалистов антивирусной лаборатории «Доктор Веб», имеющими многолетний опыт вирусного анализа.

Услуги включают анализ вредоносных файлов любой сложности, по результатам которого выдается отчет, содержащий:

- описание алгоритма работы вредоносного ПО и его модулей;
- категоризацию объектов: однозначно вредоносный, потенциально вредоносный (подозрительный), др.;
- описание алгоритмов работы вредоносного ПО, а также его модулей;
- анализ сетевого протокола и выявление командных серверов;
- влияние на зараженную систему и рекомендации к устранению заражения.

Заявки на антивирусные исследования принимаются по адресу: https://support.drweb.ru

Экспертиза вирусозависимых компьютерных инцидентов (ВКИ)

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

Экспертиза ВКИ включает:

- Предварительную оценку инцидента, объема экспертизы и мер, необходимых для устранения последствий произошедшего.
- Экспертные исследования компьютерных и других артефактов (накопителей на жестких магнитных дисках, текстовых, звуковых, фото-, видеоматериалов), предположительно имеющих отношение к ВКИ.
- Не имеет аналогов! Психологическую экспертизу личностей (персонала) с целью выявления фактов причастности к совершению / пособничеству / укрывательству / поощрению противоправных действий в отношении заказчика (комплексное определение рисков), а также фактов бездействия или халатного отношения к служебным обязанностям.
- Рекомендации по вопросам построения антивирусной системы защиты с целью недопущения ВКИ или сокращения их количества в будущем.

Полезные ссылки

Об экспертизе ВКИ: https://antifraud.drweb.ru/expertise

Заявки на экспертизу: https://support.drweb.ru/expertise

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**

Государственные сертификаты и награды, а также география пользователей Dr.Web свидетельствуют о высоком качестве продуктов, созданных талантливыми российскими программистами.

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
антивирус.рф | www.drweb.ru