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**

Dr.Web vxCube

Dr.Web vxCube — как аптечка, которая всегда под рукой. Чихнул, достал таблетку, и вперёд дальше по дороге.

Благодарный пользователь

Что делать, если компьютер в сети заражен (или у вас появились обоснованные, на ваш взгляд, подозрения, что в сети завелся «чужой») и нужно вычистить заражение полностью во всей локальной сети? На анализ вредоносных файлов требуется время, которое также необходимо на сборку обновлений, их тестирование и выкладку на серверы обновлений. Каждая отдельная операция длится недолго, но в итоге информация об актуальных угрозах безопасности (даже если не отключены обновления) не может появиться в антивирусных базах на стороне пользователя мгновенно.

Ждать обновления штатного антивируса? Но от момента совершения мошеннической операции до вывода средств в среднем проходит 1–3 минуты. 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. К тому же не каждая компания может себе позволить штатного вирусного аналитика.

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, если он будет признан вредоносным:

- изготовит лечащую утилиту для устранения последствий его работы
- выявит его обращения к локальным и сетевым ресурсам
- сообщит о созданных в системе файлах
- укажет на серверы злоумышленников

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

И не только

- Что может натворить на вашем ПК угроза нулевого часа (0-hour threat)? Вы увидите это еще до того, как она начнет действовать в реальности.
- Каковы могут быть последствия гипотетической атаки на ваше предприятие? Узнайте заранее.
- Что именно собирались делать злоумышленники в вашей сети? Dr.Web vxCube разберет досконально.

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. Технологически сложные и особо опасные троянцы, 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. Всегда существует временной промежуток между выпуском злоумышленниками не опознанного антивирусом троянца, попаданием его образца на анализ в вирусную лабораторию, изготовлением противоядия и загрузкой обновления на атакуемые компьютеры.

Хотите узнать больше о том, как противостоять неизвестным угрозам? Переходите на страницу https://training.drweb.ru/courses/admins.

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 экстренного анализа вредоносных и потенциально вредоносных файлов Dr.Web vxCube.

Dr.Web vxCube — сервис, предназначенный для анализа файлов. Вы отправляете файл (исполняемый файл, офисный документ) на анализ. Данный файл автоматически (без участия аналитиков компании, что гарантирует полную конфиденциальность его анализа) запускается в изолированном окружении.

По умолчанию проверка производится за одну минуту — ведь пользователям важно время реакции. Если исследователь считает, что времени по умолчанию недостаточно для полного анализа поведения подозрительного файла, желаемое время проверки можно задать в настройках.

В итоговом отчете пользователю сервиса предоставляются:

- Запись рабочего стола виртуальной машины с анализируемым файлом. Запустив видео, вы можете узнать, как выглядит процесс заражения (естественно, если действия программы отображаются на экране), сравнить описание данного события пользователем с реальной ситуацией.
- Оценка вредоносности. Ориентируясь на имеющиеся критерии, сервис оценивает, является ли исследуемая программа вредоносной или нет, а также насколько она может быть опасной.
- Если сервис признал исследуемый файл вредоносным, то автоматически создается утилита Dr.Web CureIt!, в базе которой содержится информация для лечения проанализированного объекта.
- Связи анализируемого файла — граф процессов с сигнатурным сканированием производных. К каким файлам были обращения, в какие верви реестра осуществлялась запись, какие ресурсы сети Интернет были использованы и так далее.
- Список изменений в системе, включая запись в элементы автозапуска, список файловых и сетевых операций. Все события фиксируются по временной шкале, что дает возможность восстановить последовательность событий, в том числе в ходе расследования ИТ-инцидента.
- Дампы созданных файлов, оперативной памяти, сетевых пакетов.
- Журнал всех вызовов WinAPI.
- Контрольные суммы исследуемого файла.
- Архив с результатами анализа.

В ходе анализа также производится проверка на вредоносность удаленных ресурсов, к которым обращается анализируемый файл: на графе процессов они помечаются красным, оранжевым или серым в зависимости от степени опасности.

Проверка проводится параллельно в разных ОС, что крайне важно для анализа событий в гетерогенных системах.

Для Android OS отчет дополнительно содержит разделы:

- «Манифест»,
- «Телефонные звонки и SMS»,
- «Намерения».

Ознакомиться с результатами предыдущих проверок можно в личном кабинете.

Dr.Web vxCube — противоядие по запросу

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.

Проверка производится на изолированных виртуальных системах на серверах компании «Доктор Веб» в окружении, задаваемом пользователем сервиса. Пользователь сервиса может указать, в каких операционных системах и с какими версиями приложений, которые, по статистике Dr.Web, сейчас больше всего атакуются злоумышленниками, должна происходить проверка.

Анализ производится в нескольких операционных системах, используются типичные приложения:

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

С этих форматов начиналось развитие проекта, с тех пор список существенно вырос/

... Добавлена поддержка форматов BAT, SLK, CHM и IQY.

... Добавлена поддержка форматов PUB, ACCDB, SCT и PS1.

... Добавлены новые правила для отслеживания поведения APK-файлов.

Вы знаете о том, что злоумышленников интересуют эти файлы? Об этом и многом другом вы можете узнать в впусках проекта «Антивирусная правДА!» https://www.drweb.ru/pravda.

Использование злоумышленниками новый типов файлов для атак не остается незамеченным Dr.Web.

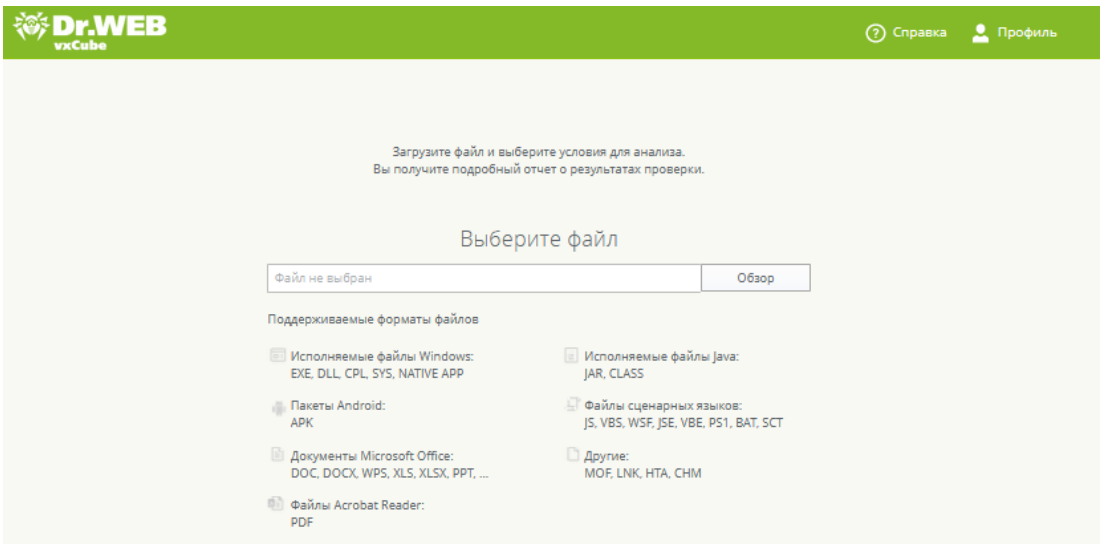
Сервис Dr.Web vxCube имеет возможность экспорта результатов анализа в машиночитаемые форматы STIX/MAEC, что позволяет легко интегрировать сервис в существующую SOC или SIEM, а также в действующую ИБ-инфраструктуру с помощью HTTP API, предоставляющего полноценный доступ ко всем функциям анализатора.

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

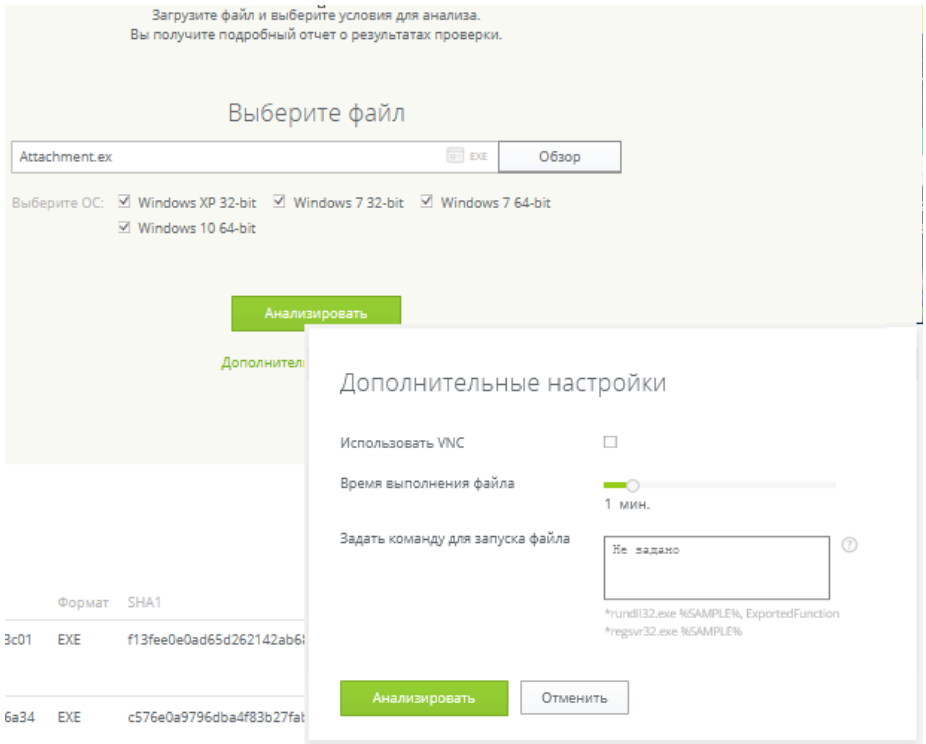
1. Пользователь получает доступ к анализатору для отправки подозрительных файлов на облачный анализ.

Для входа в сервис и отправки подозрительного объекта на анализ Dr.Web vxCube требуется только браузер и наличие интернет-подключения. Вы можете анализировать угрозу, где бы вы ни были.



В окне сервиса указан список типов файлов, которые могут анализироваться сервисом. Список постоянно расширяется.

Для каждого загруженного файла можно указать тестовую среду (для исполняемых файлов это операционная система).



Исследователь может:

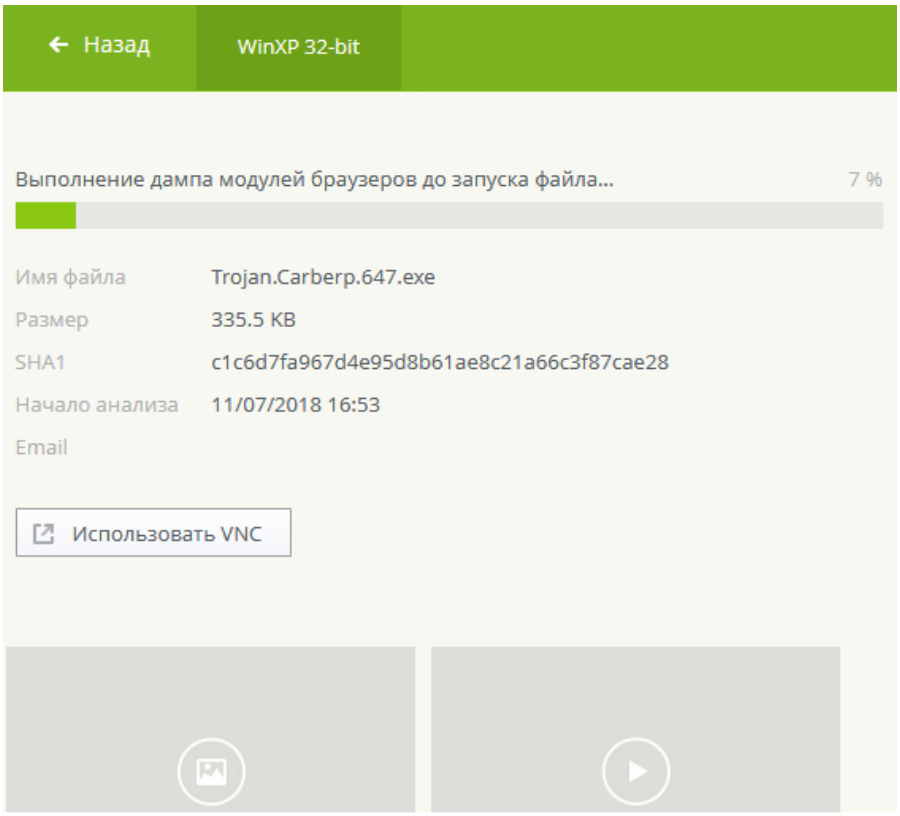
- указать, в каких операционных системах и с какими версиями приложений должна происходить проверка;
- задать желаемое время проверки в настройках, если считает, что одной минуты недостаточно для полного анализа поведения подозрительного файла;

- 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.

! Проверка подозрительного файла возможна как в ручном, так и в автоматическом режиме.

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

2. Для каждого полученного файла запускается специальная виртуальная машина, в этой виртуальной машине установлены типичные приложения, которые атакуются злоумышленниками. Анализатор запускает отправленный исследователем объект в изолированном окружении и изучает его поведение. Анализ производится автоматически, без участия вирусных аналитиков «Доктор Веб».



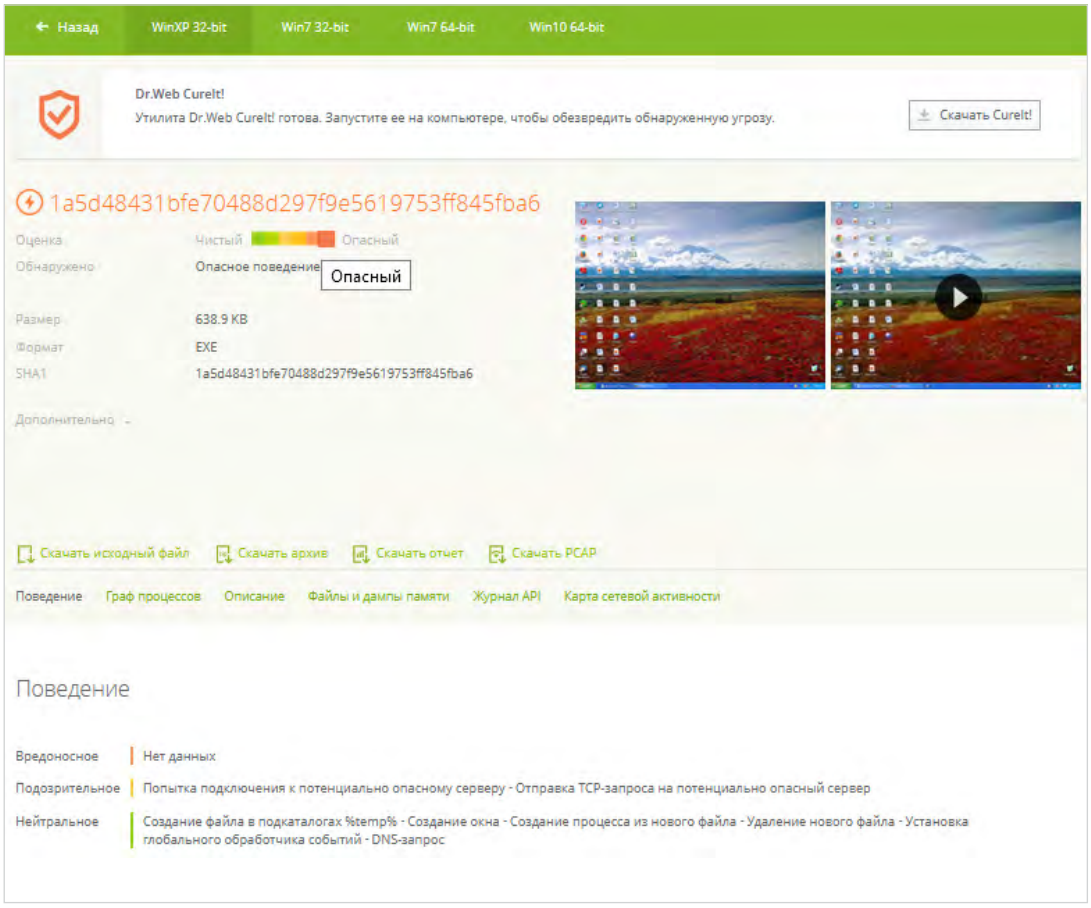
Сервис бережно относится к персональным и конфиденциальным данным согласно принципам, прописанным в политике конфиденциальности «Доктор Веб»: https://company.drweb.ru/policy. Файлы, поступившие на анализ через Dr.Web vxCube, отделяются от файлов, поступивших иными путями.

По умолчанию проверка занимает от одной минуты.

! Злоумышленники готовы к тому, что созданное ими вредоносное ПО будет анализироваться, и умеют обходить различные песочницы. Виртуальные машины, созданные в рамках проекта Dr.Web vxCube, для вредоносной программы неотличимы от реальных машин их жертв, в итоге вредоносное ПО не сможет укрыться от анализа.

По завершении анализа создается отчет. Отчет включает всю нужную для дальнейшей работы информацию об анализируемом файле. В дальнейшем отчет 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.

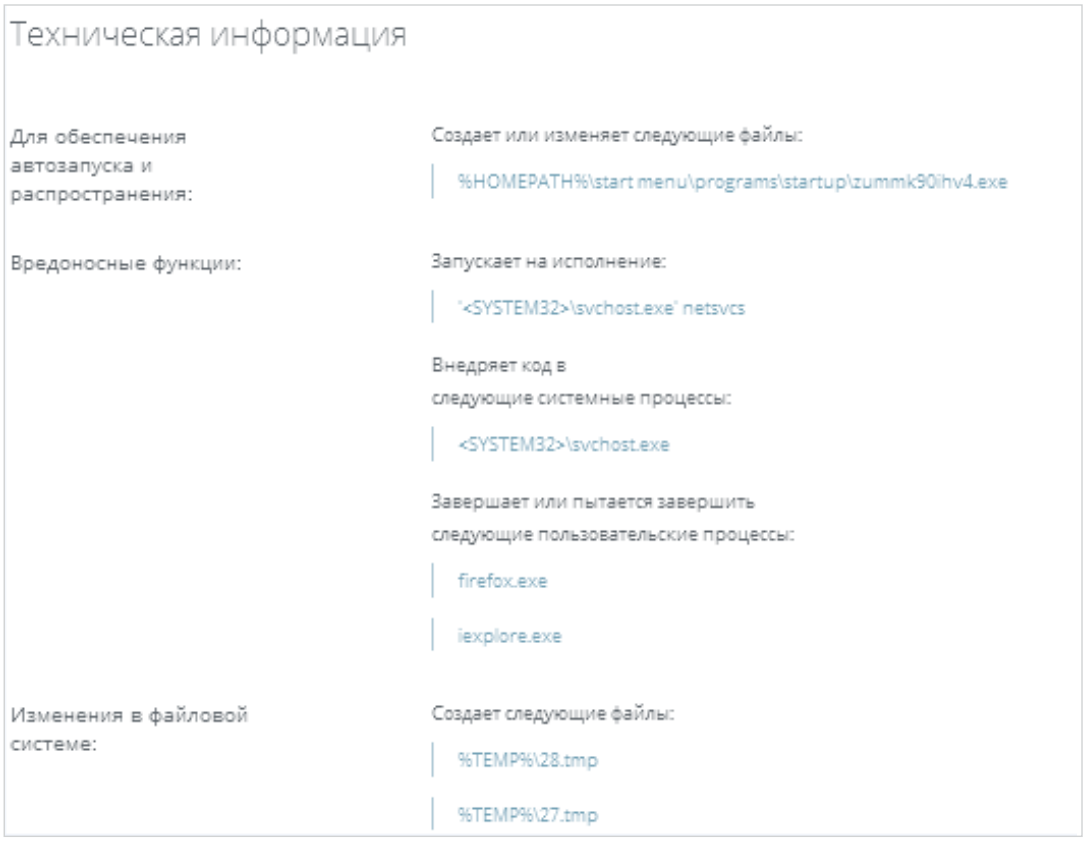


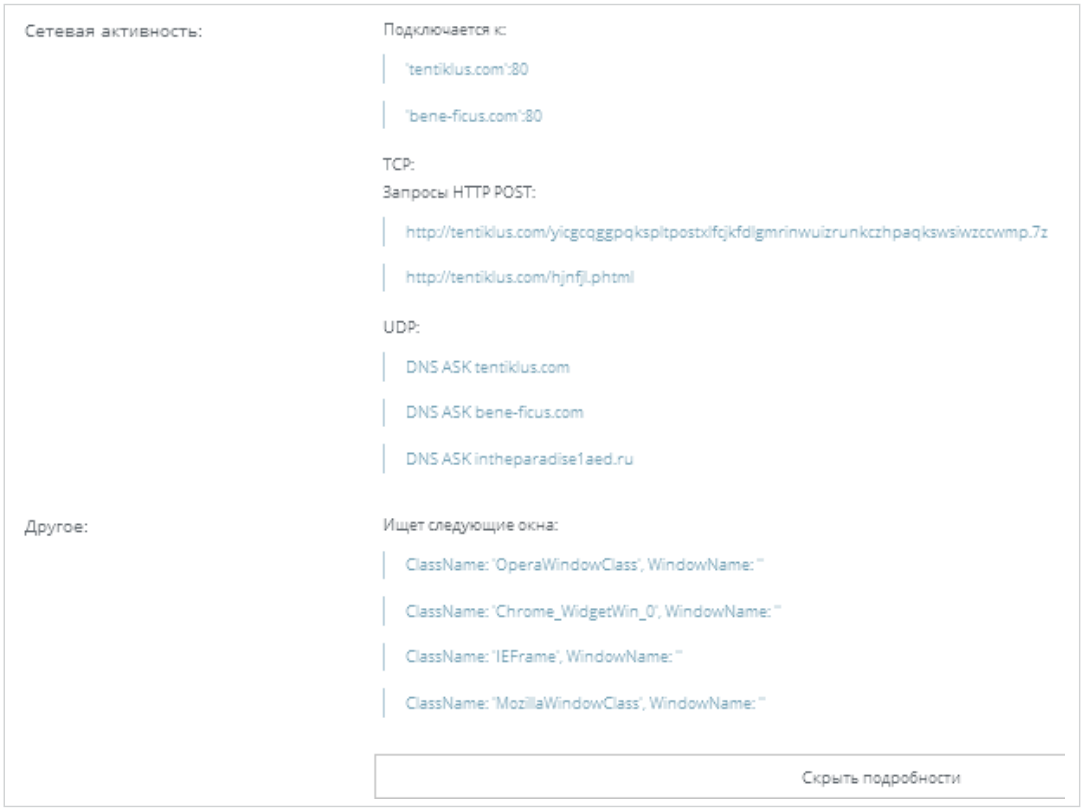
Вверху страницы отчета размещены оценка вредоносности и информация о файле, справа запись запуска и работы анализируемого файла.

Кроме того, в итоговом отчете пользователю сервиса предоставляются следующие данные.

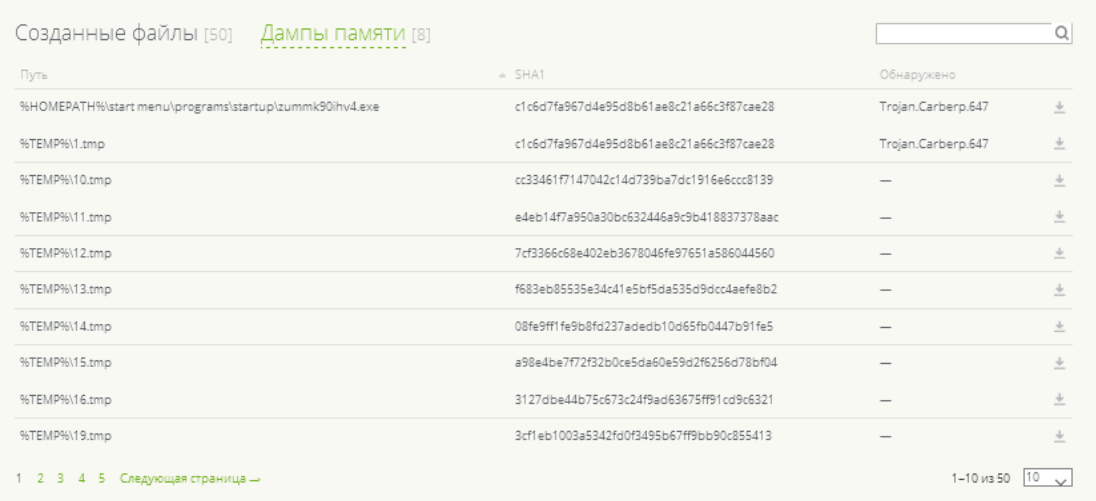
- **Связи.** Покажет, к каким файлам обращалась программа, в какие ветви реестра осуществлялась запись, какие интернет-ресурсы были использованы и т. д.

- **Техническая информация** отчета подскажет, что из системы нужно удалить, на защиту каких ее частей следует обратить повышенное внимание.

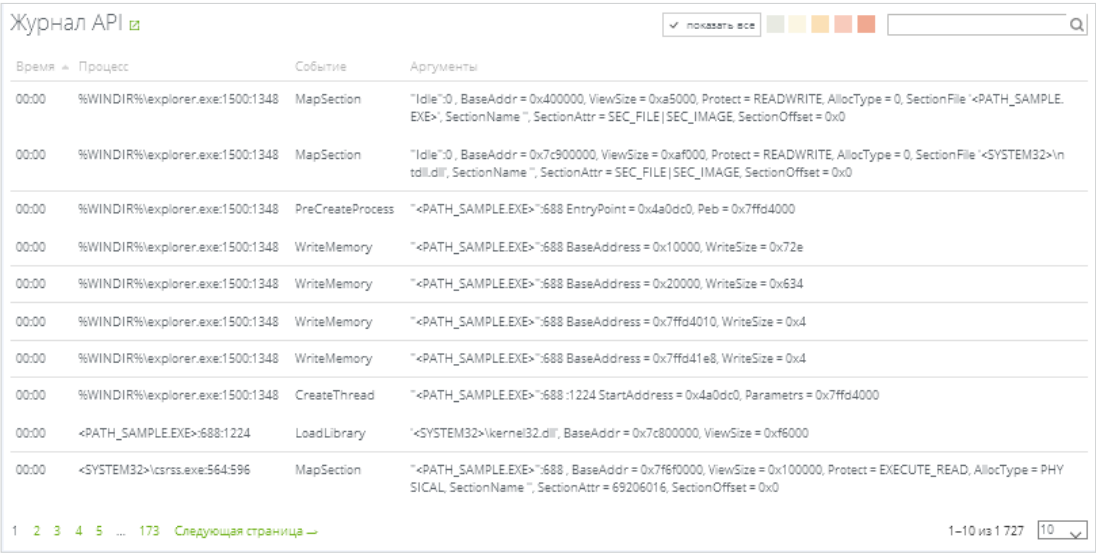




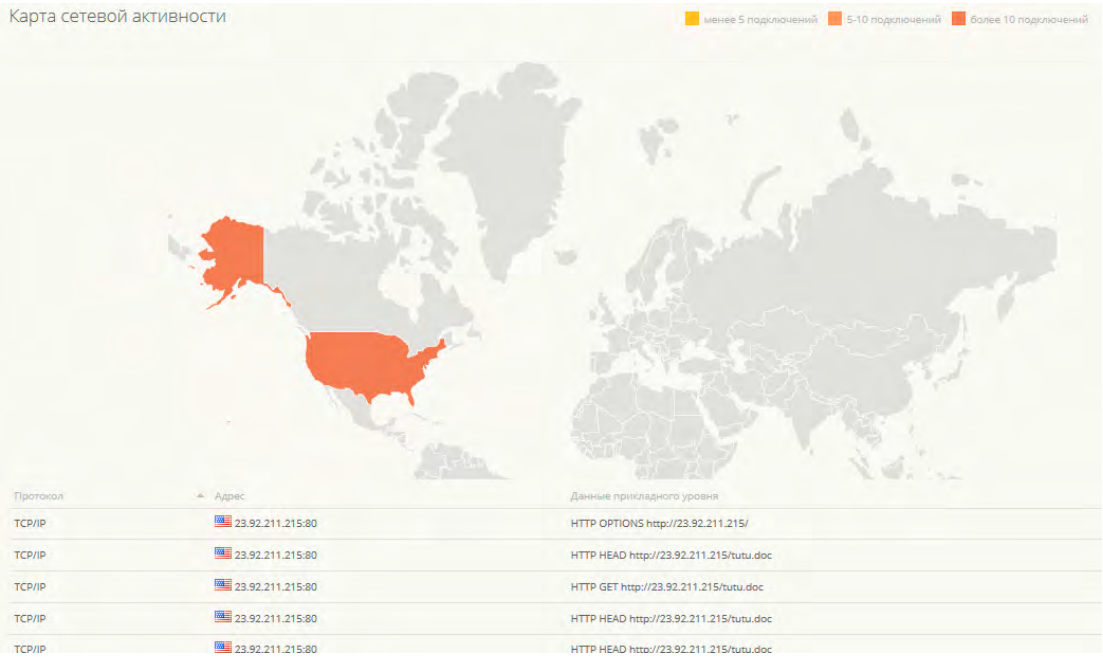
Информация о созданных исследуемым образцом файлах и их контрольных суммах позволит удалить последствия заражения.



Журнал API покажет, как вредоносная программа прячется в системе.

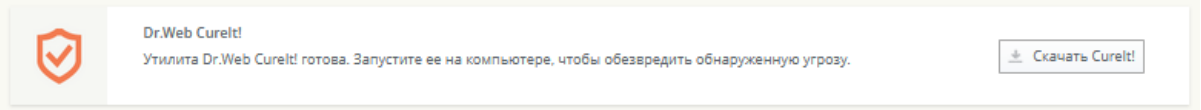


- **Карта сетевой активности**, граф процессов с сигнатурным сканированием производных, расскажет, к серверам в каких странах мира обращалась вредоносная программа.



! 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».

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

Полезные ссылки

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

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

** Если это входит в лицензию.*

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» с многолетним опытом 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.;
- 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 ФСТ ЭК 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