Dr.WEB®
Сделано в России

ЗАЩИТИ СОЗДАННОЕ

Компетенции и инструментарий «Доктор Веб»

для менеджмента компьютерных инцидентов

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

www.drweb.ru | www.антивирус.рф

Стоимость ликвидации ущерба всегда многократно превосходит инвестиции в безопасность – это, увы, аксиома. Каким образом АНТИВИРУС в самом широком смысле этого слова (включая весь комплекс сопутствующих ему сервисов и услуг) может оградить от тяжелых последствий ВКИ – расскажет наша брошюра.

Обращайтесь за квалифицированной помощью к специалистам «Доктор Веб»

Казалось бы: уже более 30 лет существуют антивирусы, в 2021 году исполнится 60 лет со дня создания первого компьютерного вируса... Но до сих пор живет ошибочная и пагубная для корпоративной ИБ модель поведения системных администраторов: этот антивирус пропустил вирус — несите новый антивирус, причем «лидер рынка». Но и он пропускает вирусы, потому что все антивирусы не без греха. Замкнутый круг?

Увы, но даже знающие специалисты в области компьютерных технологий отказываются понимать и признавать, что вирусное заражение – это не просто пропуск антивирусом очередной вредоносной программы внутрь защищаемого периметра. Это – комплекс ошибок в построении и поддержании на должном уровне системы защиты, следствие неустановленных патчей к брешам, неправильных или неиспользуемых имеющихся настроек антивируса и подчас даже цепь случайных действий участников производственного процесса, приведшая к проблеме.

Пример запроса пользователя в службу технической поддержки «Доктор Веб»:

В результате вирусной атаки часть моих данных была заархивирована и запаролена.

И выводы наших специалистов о причинах инцидента:

Произошел несанкционированный вход через подбор/похищение пароля одной из учетных записей по RDP (или через терминальную сессию).

Злоумышленник запустил легальную программу для сжатия данных, добавил данные в архивы, вручную был введен пароль на архив из длинной последовательности символов.

Есть ли в таком инциденте вина антивируса? По умолчанию тот не блокирует легальные программы – а именно их и использовал злоумышленник. Кроме того, он действовал по RDP от лица пользователя.

> Антивирус может блокировать запуск любых программ. Но указать, какую программу нужно разрешить, а какую блокировать – должен оператор антивируса.

Конечно, исследование проводились не только для обеления роли антивируса, но показало, что администратор компьютера допустил ряд промахов в настройке системы защиты. Цель исследования, которое могут провести наши специалисты, в том, чтобы столкнувшаяся с инцидентом компания, получив наши рекомендации, никогда больше не оказалась в схожей ситуации.

В любой антивирусной компании есть (или должна быть) служба технической поддержки. Антивирусные производители с серьёзным стажем на рынке — производители антивирусных программ, такие как компания «Доктор Веб» —располагают также исследовательскими центрами, или вирусными лабораториями. За этими понятными с виду словами скрываются сотни высококвалифицированных специалистов, серьёзнейшие многолетние научно-технические наработки (опыт Dr.Web

в этой области исчисляется почти 3 десятилетиями), ноу-хау, технологические открытия, патенты первопроходцев и неиссякаемая база знаний о моделях поведения всех типов вредоносных программ, инструментарии хакеров, стратегий и тактик для проникновения к золоту сегодняшних экономик — данным, информации и знаниям.

«В стоимость лицензии включена техническая поддержка» - уведомляются покупатели лицензий Dr.Web. Так что же включает в себя эта столь доступная техническая поддержка? В каких случаях компаниям полезно обратиться за ней в «Доктор Веб»?

Все пропало?

Когда атака уже произошла, ясны ее последствия и даже предприняты действия по восстановлению, наиболее важным становится принятие мер по недопущению повторения инцидента. Однако компании за малым исключением редко занимаются выяснением истинных причин произошедшего и внесением улучшений в систему безопасности. И только единицы обращаются за помощью в этом вопросе в техническую поддержку своего антивируса. Парадокс! Вместо исследования обстоятельств пропуска вируса люди предпочитают броситься искать новый, волшебный, защищающий от 100% вирусов антивирус. Но такого не существует.

Однажды проникнув в корпоративную сеть, преступник не устанет делать это снова и снова. Именно тщательное расследование причин и обстоятельств инцидента позволяет сделать невозможным или минимизировать вероятность повторения такого же или схожего сценария атаки.

Инструментарий «Доктор Веб» позволяет оказывать услуги анализа инцидентов, аудита безопасности, поиска виновников инцидента силами специалистов технической поддержки в сотрудничестве с инженерами вирусной лаборатории. Проводимые исследования – один из способов **прогнозирования будущих атак**, а предпринимаемые по итогам исследования меры — **действия на упреждение**.

Чистыми руками

То, что хакеры используют для атак только вирусы и троянцев (т. е. программы, которое обязан детектировать антивирус), — миф. Сегодняшний инструментарий хакера в обязательном порядке включает в себя как легитимные утилиты, так и программы «двойного назначения», которые могут использоваться как исследователями безопасности, так и злоумышленниками. Точно так же кухонный нож может использоваться для приготовления пищи или для убийства. Такие программы антивирус не обязан распознавать как вредоносные.

Вредоносен ли архиватор? Вполне легитимная программа. Но с ее помощью можно заархивировать с паролем данные и потребовать выкуп. Решить, можно ли запускать архиватор на данной машине, может только администратор.

А программа удаленного доступа? Ею может воспользоваться и администратор – для настройки антивируса, и хакер – для кражи данных.Это – программа двойного назначения, в руках злоумышленника она может стать опасным ПО. По умолчанию ее запуск разрешен, но, опять же, решить, какие программы можно запускать, а какие – нет, должен администратор. Либо он может полностью запретить запуск потенциально опасных программ, но мало кто делает так.

В системах, которые исследовали наши специалисты, встречались и «кряки» к пиратскому ПО (разумеется, зараженные), и неизвестные антивирусы. В лучшем случае все это тормозило и блокировало друг друга.

Система должна быть чиста как капля росы – в ней не должно быть ничего лишнего.

Нет дыма без огня?

В ИТ и такое бывает. Миф о том, что вирусное заражение можно распознать всегда, — живучий и вредный. Да, необходимость отказа от этого заблуждения больно бьет по самолюбию ИТ-специалиста, но такова реальность. Многие сегодняшние киберпреступники научились успешно прятать следы своего присутствия, и только внимательный и скрупулёзный вирусный аналитик, точно знающий, как и где скрывается злоумышленник, может его изобличить. Игра в прятки хакера с сисадмином может длиться годами, и компания может даже не подозревать, что все ее секреты давно известны посторонним. Поэтому, если вы владеете ценными данными, если для вас важна репутация в глазах клиентов и партнеров, если вы обмениваетесь данными с чувствительными ИТ-системами (ГИС/МИС и подобными) и уж тем более если в вашем ведении находится управление ИТ-инфраструктурой объекта КИИ — в числе рутинных мероприятий отдела ИБ вашей компании обязана быть профилактика ВКИ. Такие периодические исследования состояния ИБ системы также может проводить для вас служба технической поддержки «Доктор Веб». Они особенно важны, если ваша компания располагает информацией, за которой охотятся конкуренты и злоумышленники.

Конечно, это антивирус виноват!

Бывают инциденты, когда все признаки заражения налицо, и пользователь твердо уверен в том, что сплоховал антивирус, но...

Пример запроса пользователя в службу технической поддержки «Доктор Веб»:

Несанкционированный вход в компьютер с удалением ВАЖНОЙ ИНФОРМАЦИИ – файлов 10 Гб

Выводы наших специалистов о причинах инцидента:

С жестким диском наблюдаются проблемы, судя по многочисленным сообщениям системного журнала о неверном блоке на устройстве \Device\Harddisk1\DR1, что может вызвать различные проблемы и нестабильную работу

Или другой пример запроса:

При старте системы Антивирус не запускается и находится в постоянной загрузке. При попытке запустить сканер появилось окно с сообщением об ошибке 1722.

Выводы:

Судя по отчету Ваш диск находится в аварийном состоянии. Я бы рекомендовал в первую очередь скопировать все важные данные с этого диска в надежное место, на другой диск или в облако.

Затем заняться его диагностикой или заменой. О нормальной работе антивируса, да и в целом любого приложения на таком диске не может быть и речи.

Еще пример:

Запускаю на ноутбуке Асус полное сканирование, но отсканировать в полном объеме не получается. Ноутбук отключается ещё до окончания проверки. Изначально была операционка виндовс 7, сейчас виндовс 10. Быстрая проверка вирусов не находит.

Вывод:

Все симптомы указывают на то, что система перегревается, и срабатывает защита от перегрева.

Мы и такое определить можем – и не надо бросаться искать новый, лучший антивирус.

Чем поможет «Доктор Веб»

«Доктор Веб» имеет богатый инструментарий средств, с помощью которых мы можем исследовать причины инцидента и выработать рекомендации по устранению его последствий, или провести профилактическую проверку технического «здоровья» вызывающей подозрения системы.

Dr.Web FixIt!

Это облачный сервис для удаленной диагностики инцидентов ИБ (вирусных инцидентов, возможных целевых атак и нарушений правил ИБ) и устранения их последствий. Он будет особенно полезен тем компаниям, которые не могут позволить себе собственные SOC-команды или если квалификация системных администраторов не позволяет грамотно анализировать вирусозависимые компьютерные инциденты.

Использование Dr.Web FixIt! позволит компании существенно экономить на расходах на такой персонал.

Задачи, решаемые Dr.Web FixIt!

- Анализ состояния безопасности устройств, поиск и удаление вредоносного и потенциально опасного ПО и остаточных следов произошедшего заражения.
- Анализ подозрительного поведения системы на предмет выявления предположительных заражений и, возможно, произошедших или действующих до сих пор целевых атак.
- Поиск нарушений правил и политик ИБ компании.
- Анализ причин произошедших заражений и других инцидентов ИБ.

Диагностическая утилита Dr.Web FixIt! собирает данные, проводит их первичный анализ и выдает результат в пригодном для дальнейшего анализа виде. Она способна выявлять именно следы присутствия вредоносных программ, снимает «слепок» состояния информационной безопасности системы, исследовав:

- установленные программы и обновления;
- запущенные и запускаемые процессы;
- подозрительные записи в реестре и их связи с другими объектами;
- установленные драйверы и расширения браузеров;
- модули, загруженные в процессы;
- секторы жестких дисков, использованные злоумышленниками, и многое другое.

В случае выявления ВПО создается специфическая для условий конкретной зараженной системы *лечащая* утилита Dr.Web FixIt! для устранения последствий заражения. После чего система исследуется снова — столько раз, сколько нужно для полного устранения всех последствий инцидента.

Необходимо отметить, что сервис позволяет не только выявить заражение на текущий момент, но и при необходимости произвести ретроспективный анализ состояния защиты системы, проследить во времени ситуацию и поведение критических сервисов и программ. Это может оказаться полезным для обращения в правоохранительные органы или для доказательства невиновности в инциденте сотрудников компании и ее руководства.

В отличие от лечащей утилиты Dr.Web CureIt!, предназначенной для обнаружения уже известных или похожих на известные вредоносных программ с помощью вирусных баз, Dr.Web FixIt! предназначен для выявления новейших вредоносных программ, еще не попавших в руки аналитиков, а также программ, используемых для целевых атак и не выявляемых никакими иными инструментами. И не только. Dr.Web FixIt! помогает выявить случаи использования злоумышленниками легитимных инструментов, оценить состояние системы, наличие уязвимостей и многое другое. Dr.Web

FixIt! – это в первую очередь средство аудита устройства, в отличие от Dr.Web CureIt! и антивирусов, предназначенных для очистки системы от известных вредоносных программ. Dr.Web FixIt! может использоваться для удаления последствий заражения. И каждый раз это специальная сборка утилиты под конкретную ситуацию, а не жестко прошитые в вирусных базах действия антивируса. Она выполняет только тот набор инструкций, который был подготовлен по результатам анализа отчета диагностической утилиты, поэтому каждая сборка Dr.Web FixIt! – уникальна. Точечная операция хирурга вместо ковровой бомбардировки. Dr.Web FixIt! может находить вредоносные и подозрительные объекты, выявлять ошибки в настройках и проблемы с жестким диском с помощью специальных правил, фактически выполняя роль помощника аналитика, готовящего данные для анализа и принятия решения.

Использование Dr.Web FixIt! не зависит от использования антивирусных решений Dr.Web. Dr.Web FixIt! могут применять пользователи любых средств защиты.

Есть одно «но»: в руках неспециалиста по вопросам компьютерных заражений и атак Dr.Web FixIt! – малоинформативный инструмент. Поэтому у нас предусмотрено два вида лицензий для компаний — корпоративная и гибридная. Это позволяет либо организовать процесс расследования инцидента с привлечением команды аналитиков «Доктор Веб», либо сосредоточиться на задачах исследования инцидентов силами собственных специалистов клиента. При этом, даже если для решения проблем используется собственная команда, всегда есть возможность привлечения специалистов «Доктор Веб» на платной основе.

! Ни один отчет не может быть проанализирован автоматически так глубоко и исчерпывающе, как это может сделать опытный вирусный аналитик. Правильные выводы из данных отчета и решения о том, как действовать дальше, способен сделать только профессионал своего дела. Именно компетенция специалистов «Доктор Веб», а также наша экспертиза позволяют в сырых данных отчета разглядеть злой умысел и выявить его причину — даже там, где для совершения инцидента не было использовано вредоносное ПО.

Dr.Web vxCube

Для тех, кто не имеет времени ждать и знает, как действовать самостоятельно

Если в вашей компании есть специалисты, способные среди массива данных определить, что тот или иной файл предположительно может являться угрозой для ИБ, убедиться в правильности предположения поможет облачный сервис анализа вероятных угроз Dr.Web vxCube. Он существенно повышает скорость реагирования на вероятные и новые угрозы, не распознаваемые антивирусами.

Dr.Web vxCube – это облачный интеллектуальный интерактивный анализатор подозрительных объектов для специалистов по информационной безопасности и киберкриминалистов. Вы отправляете файл (исполняемый файл, офисный документ) на анализ. Файл автоматически (без участия аналитиков «Доктор Веб», что гарантирует полную конфиденциальность его анализа) запускается в изолированном окружении. При этом используются техники, препятствующие вредоносному ПО распознать аналитическое, а не реальное окружение, и затаиться, отказаться от проявления своей вредоносной сущности.

Dr.Web vxCube:

- выявит обращения ВПО к локальным и сетевым ресурсам;
- если файл будет признан вредоносным, изготовит лечащую утилиту для устранения последствий его работы и укажет на серверы злоумышленников;
- сообщит о созданных в системе файлах, использованных ресурсах.

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

В результате анализа исследователь получит:

- запись рабочего стола виртуальной машины с анализируемым файлом;
- оценку вредоносности;
- связи анализируемого файла;
- список изменений в системе, включая запись в элементы автозапуска, список файловых и сетевых операций;
- дампы созданных файлов, оперативной памяти, сетевых пакетов;
- журнал всех вызовов WinAPI;
- контрольные суммы исследуемого файла.

Существует возможность интеграции Dr.Web vxCube с внутренними системами компании (SOC/SIEM) и получения автоматического ответа о вредоносности файла — в том числе из Dr.Web Enterprise Security Suite.

Подробнее

Экспертиза ВКИ

С 2012 года

Цифровизация так же неизбежна, как и смена времен года. Одним из попутных ее аспектов уже становится ужесточение административной и уголовной ответственности для руководителей предприятий и служб ИБ, а также их сотрудников за умысел, бездействие или халатность при организации защиты информационной структуры предприятия, из-за которых могут произойти:

- хищение (денег или данных) компьютерными устройствами, принадлежащими предприятию или с личных устройств сотрудников, используемых для работы;
- распространение вредоносных программ и заражение информационных сред других предприятий и компаний;
- использование информационной структуры предприятия для незаконной предпринимательской деятельности или для целей шпионажа или терроризма;
- проникновение на критические и инфраструктурные объекты через устройства компании;
- ненадлежащая идентификация участников коммуникаций в бизнес-процессах предприятия, в результате чего возможны факты мошенничества;
- сокрытие фактов ВКИ, что особенно критично для операторов объектов КИИ и ИСПДн.

Поэтому потенциально любой инцидент в компьютерной системе – это не просто простои или ущерб репутации, не только внутреннее дело компании. Это еще и возможное уголовное преследование. Чтобы обезопасить компанию от возможных катастрофических последствий судебного разбирательства, защитить ее доброе имя, оправдать невиновных сотрудников или изобличить злоумышленника, компании может потребоваться экспертиза компьютерного инцидента. «Доктор Веб» оказывает и такие услуги.

Экспертные исследования компьютеров и их содержимого (жестких дисков, текстовых, звуковых, фото-, видеоматериалов), предположительно имеющих отношение к ВКИ, производятся с соблюдением требований УПК РФ и ГПК РФ.

Уникальность экспертизы «Доктор Веб» состоит в том, что помимо физического исследования системы, используемой для свершения преступления, мы также можем проводить психологическую экспертизу личностей (персонала) с целью выявления фактов причастности к совершению/пособничеству/укрывательству/поощрению противоправных действий в отношении заказчика (ком-

плексное определение рисков), а также фактов бездействия или халатного отношения к служебным обязанностям.

Также по результатам экспертизы мы можем выдавать рекомендации по вопросам построения системы антивирусной защиты с целью недопущения или сокращения числа ВКИ в будущем.

Что обеспечивает высокий уровень экспертизы ВКИ компании «Доктор Веб»?

- Собственная антивирусная лаборатория. Знание современных вирусных угроз, их постоянный мониторинг и изучение, наличие собственных методик их обнаружения (детектирования).
- Наличие в штате сотрудников с особой квалификацией, имеющих многолетний опыт проведения экспертиз.
- Наличие специального программного обеспечения и оборудования для снятия информации в соответствии с установленными процедурами для обеспечения доказательной базы в суде.
- Исследовательская группа антивирусной лаборатории, ведущая «интернет-разведку».
- Специалист-профайлер, умеющий создавать профили преступников, а также с возможностью поиска инсайдеров среди сотрудников компании.

Специалисты «Доктор Веб» в рамках договора об экспертизе обеспечивают:

- Съем информации с машинных носителей в порядке, обеспечивающем предъявление их в качестве доказательств судебным органам;
- Поиск информации на машинном носителе, средстве вычислительной техники, образе, полученном с машинного носителя о действиях пользователя, злоумышленника или вредоносной программы. В том числе информации об используемых файлах, действиях с ними, запускаемых процессах, используемых ресурсах локального компьютера и Интернета. Установление фактических обстоятельств совершения тех или иных действий, истинной причины произошедшего.
- Определение возможности совершения каких-либо действий с помощью средств вычислительной техники, программного обеспечения, найденного на машинном носителе или его образе.
- Исследование и описание использованных злоумышленниками инструментов и методик. Определение назначения и возможностей найденного программного обеспечения, в том числе возможностей, предоставленных злоумышленнику.
- Выявление компьютеров и серверов, вовлеченных в инцидент.
- Ретроспективный анализ инцидента.

В случае необходимости может осуществляться выезд на место для выявления затронутых инцидентом устройств и носителей информации, корректного копирования данных, в том числе с помощью криминалистического оборудования, для их последующего анализа.

По результатам анализа заказчику предоставляются корректно оформленные цифровые свидетельства и экспертное заключение. При необходимости производится лечение пораженных систем с помощью специально созданных под конкретные условия лечащих утилит.

Подробнее

Практика показывает, что наш опыт и применяемый инструментарий позволяет выявлять самые сложные и затяжные атаки (т. н. APT-атаки), в том числе длящиеся годами, восстанавливать картину событий, находить источники проникновения и делать выводы о причинах произошедшего, как, например, в случае атаки на государственные учреждения двух стран СНГ.

> *В ходе расследования было установлено, что сетевая инфраструктура учреждения была скомпрометирована как минимум с декабря 2017 года.*
>
> *...Анализ показал, что, как и в предыдущем случае, заражение началось задолго до обращения — в марте 2017 года.*

Источник

Иногда экспертиза ВКИ помогает изобличить виновника инцидента, а иногда – оправдать невиновных.

Примеры наших экспертиз

Другие услуги «Доктор Веб»

- Исследования и описания ВПО

Подавляющее большинство вредоносных программ даже не попадает в руки аналитиков и обрабатывается, например, методами машинного анализа. Что делает вредоносная программа, какой функционал в нее заложен – ему неважно. Но, в отличие от антивируса, пользователям зачастую важно знать, на что именно способна обнаруженная у них программа – что хотел сделать злоумышленник. Именно всестороннее исследование ВПО позволяет ответить на вопрос о целях киберпреступников.

В таком случае у нас можно заказать подробное исследование и описание явных и потенциальных возможностей ВПО. Услуги включают анализ и описание вредоносных файлов любой сложности, по результатам чего выдается отчет, содержащий:

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

Это может понадобиться компании и для обращения в правоохранительные органы.

Такая услуга входит в некоторые пакеты поддержки. Также можно заказать подобные исследования отдельно, обратившись в службу поддержки «Доктор Веб». Дополнительно можно заказать составление списка мер по недопущению повторения инцидента.

Консультации SOC/CERT

Мы готовы делиться опытом, накопленным за почти три десятилетия разработки Dr.Web и исследований ВПО. Сотрудники «Доктор Веб» могут как проводить анализ предоставленной информации по запросу, так и консультировать по набору мер, которые необходимо немедленно предпринять для локализации инцидента, выявления его причин, минимизации возможного ущерба, устранения брешей в инфраструктуре, мерам, которые необходимо предпринять в дальнейшем для избежания повторения инцидента. Мы также помогаем в подготовке технических обоснований применения тех или иных средств и мер ИБ для вышестоящего руководства с целью их последующего внедрения.

Почему Dr.Web

- Разработка и поддержка — в России.
- Опыт защиты клиентов разного масштаба — от всех устройств государственных учреждений отдельных регионов России до компьютерной сети Министерства обороны России и ГАС «Выборы».
- Постоянный анализ деятельности известных кибергруппировок и используемых ими техник и инструментов с целью выявления готовящихся атак. Превентивное внедрение в продукты компаний технологий, парирующих использование кибергруппировками находящихся в их разработке инструментов.
- Глубокое знание операционных систем и ПО аппаратной части ЭВМ.
- Умение предвидеть пути эволюции ВПО.
- Развитая система круглосуточного сбора предположительно вредоносного ПО (Threat Hunting Tricks). Машинные методы обработки большого массива собранного ВПО.

- Автоматизированный круглосуточный выпуск обновлений вирусных баз, многократно ускоряющий процесс доставки обновлений пользователям. Тщательные методики тестирования обновления с целью недопущения ложных срабатываний.
- Постоянное развитие базовых антивирусных технологий, зарекомендовавших себя как эффективные (WannaCry, от которого не пострадал ни один пользователь Dr.Web, был отловлен эвристическим анализатором, который разрабатывается с 1994 года!).
- Разработка новых прогрессивных антивирусных технологий, в том числе основанных на методах машинного обучения.

Подробнее

«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.

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