Dr.WEB®
с 1992 года

Почему нужна фильтрация корпоративной почты серверными антивирусами Dr.Web

- Получила по ел почте запрос на отчет по бухгалтерии, загрузила файл, открыла архив.
- Необдуманно открыл зип папку который пришел по эл.почте.
- Получил письмо на э-почту, загрузки и открыл «Информация о заказе 08-18-11-2019.xls».

Обращения в техническую поддержку «Доктор Веб»

Почта — основной источник распространения вредоносных программ и средство для заражения сети компании

Как правило, троянцы попадают на компьютер в результате каких-либо действий пользователей — например, отключивших антивирус вопреки политике компании и затем перешедших по ссылке из письма или открывших вложение. Даже простое открытие письма уже может дать информацию злоумышленникам о существовании конкретного почтового адреса в компании — и стать отправной точкой целевой атаки.

Антивирус и антиспам на почтовом сервере — гарантия соблюдения политик безопасности компании и защита от компрометации на уровне станции локальной сети

Компании не понесли бы убытки, если бы использовали антивирус Dr.Web на почтовом сервере, и пользователи, не получив письмо от злоумышленников, не имели бы возможности его открыть или переслать другому сотруднику или даже партнеру.

Всё, что входит в компанию и выходит из компании через почту, должно проверяться — ДО ПОПАДАНИЯ на компьютеры и устройства пользователей.

Пользователь просто не должен получить зараженное письмо.

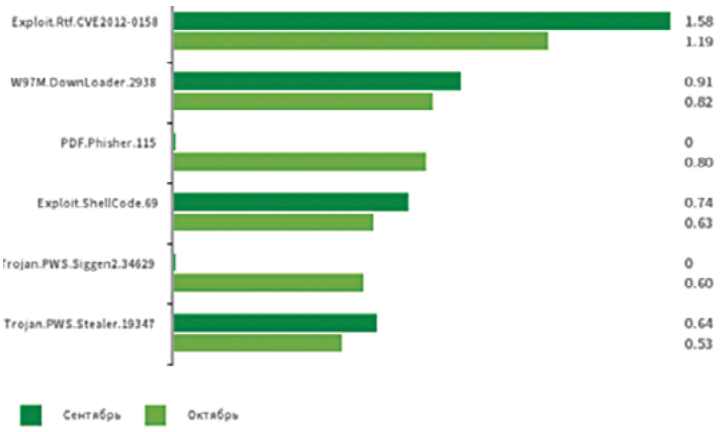
Серверный антивирус Dr.Web для почтовых серверов способен*:

- MS Exchange Linux фильтровать на сервере как внешнюю (входящую и исходящую), так и внутреннюю почту на вирусы и спам — как на контролируемом компанией сервере, так и на арендуемом;
- MS Exchange Linux фильтровать почту на шлюзе, т. е. изолировав сам почтовый сервер от сети Интернет;
- MS Exchange проверять хранящиеся на сервере почтовые сообщения на присутствие ранее не обнаруженных угроз;
- MS Exchange Linux реализовать различные политики для различных групп пользователей;
- Linux реализовать возможность глубокого анализа статистики по отправителям и получателям;
- Linux реализовать возможность фильтрации почтовых сообщений как по содержимому письма, так и по его отправителям, получателям, типам вложений;
- Linux использовать серые списки сети Интернет для фильтрации спам-рассылок;
- MS Exchange Linux помещать отфильтрованную почту в карантин для последующего ее анализа;
- Linux восстанавливать сообщения, случайно или намеренно удаленные сотрудниками из почтовых ящиков и тем самым позволять проводить расследования, связанные с утечкой информации.

** Возможности решений, входящих в группу продуктов Dr.Web Mail Security Suite, зависят от используемого в компании почтового сервера.*

Злоумышленники не только пытаются запустить на компьютерах компании различные варианты троянцев-шифровальщиков. Два места из пяти в списке наиболее активно рассылаемых вредоносных программ направлены на кражу паролей и конфиденциальной информации. Эти данные могут быть проданы или использованы для иных атак на компанию — ведь, как известно, зачастую пользователи используют одни и те же пароли для доступа ко всем ресурсам.

Статистика вредоносных программ в почтовом трафике (октябрь 2019 года)



Exploit.Rtf.CVE2012-0158 — вредоносный документ Microsoft Office Word, использующий уязвимость CVE2012-0158.

W97M.DownLoader.2938 — семейство троянцев-загрузчиков, использующих в работе уязвимости документов Microsoft Office.

Exploit.ShellCode.69 — вредоносный документ Microsoft Office Word, использующий уязвимость CVE-2017-11882.

Trojan.PWS.Siggen2.34629, Trojan.PWS.Stealer.19347 — вредоносные программы для хищения паролей и другой конфиденциальной информации.

https://news.drweb.ru/show/?i=13519

Пользователи локальной сети:

- работая с корпоративной почтой на личных компьютерах и устройствах, не используют средства защиты или отключают их;
- задерживают установку уведомлений и не перегружают компьютеры для завершения процедуры обновлений длительное время. Exploit.Rtf.CVE2012-0158 в 2019 году использует уязвимость, о которой стало известно в 2012 (!) году;
- не обновляют вовремя средства защиты на собственных компьютерах (в том числе при работе из дома), в результате чего средства защиты не могут эффективно выполнять свои функции.

Судя по отчету, антивирусные базы обновляются реже, чем выпускаются, так на момент сбора отчета 06-06-2019 базы от 2019-06-05 (13:33)

Результат анализа инцидента, связанного с заражением локальной сети в результате открытия пользователем почтового сообщения

Установка антивируса на почтовом сервере, находящемся под полным контролем специалистов по безопасности, позволяет не допустить на компьютеры пользователей письма злоумышленников, злоумышленники не получат возможности использовать приемы социальной инженерии для атаки компании.

Мобильные сотрудники, сотрудники, работающие с личных устройств, не будут иметь возможность отправить зараженное письмо клиентам компании

Киберпреступники:

- имеют возможность создать уникальную сборку для каждой отдельной жертвы;
- могут использовать для маскировки уже известного кода обфускацию, шифрование, использовать бесфайловые методы хранения и запуска;
- используют автоматизированные сервисы создания и тестирования образцов вредоносных программ.

В результате использования автоматизированных сервисов злоумышленники имеют возможность создавать новые варианты уже известных вредоносных программ чаще, чем обновляются антивирусные базы обычного антивируса. В результате атака на компанию может проводиться с использованием вредоносной программы, которая уж получена на анализ и сведения о которой уже есть в антивирусных базах, но они еще не получены в ходе запланированного обновления.

Dr.Web для почтовых серверов — это не только модуль антивируса

Антиспам, используемый в составе Dr.Web для потовых серверов, даже без помощи антивирусного ядра отфильтровывает более 90% процентов вредоносных программ, защищая наших клиентов даже от новейших вредоносных программ.

Антиспам Dr.Web работает на основе правил и эффективно удаляет из почтового трафика фишинговые сообщения с вредоносными программами — временно неопределяемыми традиционными антивирусными технологиями

Антиспам Dr.Web:

- поставляется в составе единого решения (а не в виде отдельного продукта);
- устанавливается на одном сервере с продуктом для фильтрации вирусов.

Это упрощает администрирование и обеспечивает более низкую совокупную стоимость, чем при покупке решений конкурентов.

Преимущества антиспама Dr.Web

- Не требует обучения и начинает эффективно работать с момента установки — в отличие от антиспамов, построенных на использовании алгоритма Байеса.
- Вынесение вердикта спам / не спам не зависит от языка сообщения.
- Позволяет задавать различные действия для разных категорий спама.
- Использует собственные черные и белые списки, что делает невозможным компрометацию компаний через злонамеренное внесение их в списки нежелательных адресов.
- Допускает малое количество ложных срабатываний.

Штатная работа радиостанций и безотказность процессов — это наше первое правило. Это касается и защищенности наших почтовых серверов. Использование Dr.Web Mail Security Suite значительно повысило надежность нашей системы.

Александр Суганов,
руководитель отдела системного администрирования ООО «ГПМ Радио»

- Администраторы почты жалуются, что с их двух компьютеров произведена сегодня несанкционированная рассылка по каким-то адресам.
- Администраторы опасаются, что при запланированной рассылке пользователям корпоративной почты (проводится часто, сегодня в том числе) с их ПК может быть отправлено вредоносное ПО.
- В ... произошло несколько случаев взлома п/я компании с последующей рассылкой с них спама.
- Нечто запустилось с моим письмом самому себе из Outlook 2010. Никаких писем не открывал.

Обращения в техническую поддержку «Доктор Веб»

Утечка паролей, запуск пользователем вредоносной программы или использование злоумышленником неизвестных уязвимостей — и на компьютере «поселяется» вредоносная программа, занимающаяся рассылкой спама или вредоносных почтовых сообщений по адресной книге. Не допустить попадания таких сообщений сотрудникам компании могут антивирус и антиспам, установленные на сервере компании.

Современные пользователи работают из дома и на отдыхе. Менеджер должен быть на связи всегда! Но при этом их личные компьютеры и устройства, как правило (в 60% случаев!), не защищены и часто заражены. Серверный антивирус не позволит сотруднику переслать зараженное письмо вашему партнеру или клиенту.

Вам важна ваша репутация?

Почту надо фильтровать комплексно

Использование антивируса без антиспама:

- приводит к попаданию компаний в спам-списки, в результате чего получение почты может быть заблокировано почтовыми серверами фирм-партнеров и клиентов, пострадает репутация компании как надежного партнера, заботящегося о безопасности;
- снижает производительность труда всех сотрудников компании, получающих почту и вынужденных заниматься чисткой ящиков от спама;
- позволяет хакерам проводить фишинговые спам-атаки на почтовые серверы компании и почтовые клиенты ее сотрудников; в некоторых случаях факта получения письма достаточно для заражения машины или нарушения ее работоспособности;
- приводит к повышению платы за трафик;
- приводит к повышению непродуктивной паразитической нагрузки на почтовые серверы.

С антивирусом Dr.Web почта будет отфильтрована один раз на сервере, а не несколько раз на каждой станции — это улучшит их быстродействие, и сотрудники станут значительно реже жаловаться на «тормоза» на рабочих ПК.

Благодаря использованию антиспама в Dr.Web Mail Security Suite непродуктивная паразитная нагрузка на почтовый сервер снизится (количество спама в почтовом трафике составляет до 98%, и его отсев благоприятно скажется на работе почтового сервера). Задержки в доставке почты и потерянные письма станут редким явлением!

Нашим аналитиком установлено, что заражение других ЭВМ происходило с этого почтового сервера

Результат анализа инцидента сотрудниками компании «Доктор Веб».

Получив доступ на сервер компании, злоумышленники могут сделать все что угодно. Зашифровать данные компании — и потребовать выкуп, скопировать их и продать. Троян может добавить роль для почтового сервера MS Exchange и с помощью нее изменять почтовые сообщения или копировать из них нужную им информацию — уже после того, как сообщения проверит почтовый антивирус.

Кроме защиты почтового трафика, необходимо использовать и защиту самого сервера — на уровне его файловой системы

- Только защита самого сервера и каналов коммуникаций с ним (как внутренних, так и внешних) сможет защитить его от превращения в источник распространения инфекций при проникновении в сеть неизвестного вируса.
- Защита нужна любому серверу — как расположенному внутри помещений компании, так и арендуемому внешнему серверу.

Технические последствия заражения сервера	**Коммерческие последствия заражения сервера**
▪ Уничтожение данных компании, как хранящихся на сервере, так и доступных с него. ▪ Блокирование деятельности почтового сервера, в том числе шифрование данных. ▪ Отказ в обслуживании — отключение предприятия от сети Интернет или внесение в черные списки за рассылку спама в случае попадания в бот-сеть. ▪ Снижение производительности сервера или его полная неработоспособность (простои). ▪ Повышение нагрузки на внутреннюю сеть, снижение производительности сетевых ресурсов и пропускной способности каналов. ▪ Увеличение затрат на ИТ-инфраструктуру (оплата паразитного трафика / увеличение количества серверов / затраты на хранение почты, в том числе и спама).	▪ Нарушение бесперебойности бизнес-процессов: ✓ задержки в выполнении обязательств компании перед клиентами; ✓ уход клиентов — отказ от услуг компании; ✓ задержки в выполнении сотрудниками должностных обязанностей; ✓ блокирование получения почты партнерами за счет внесения компании в черные списки. ▪ Ухудшение репутации в глазах потребителей и партнеров, в том числе за счет распространения мнения о компании как о технологически отсталой.

Правильное решение: Dr.Web Server Security Suite + Dr.Web Mail Security Suite

Скидка 20% при покупке двух продуктов

- 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.
- Windows Имеющиеся в составе Dr.Web Server Security Suite для Windows технологии превентивной защиты защитят даже от еще не известных угроз и эксплойтов, попыток связи удаленно управляемых вредоносных объектов с сервером злоумышленников (для управления ботнетами и шпионажа) — без зависимости от вирусных баз и частоты их обновлений.
- Windows Если злоумышленник не имеет полных прав на атакуемом компьютере, не имеющий аналогов на рынке модуль самозащиты Dr.Web SelfPROtect не позволит вывести антивирус Dr.Web из строя и получить контроль над сервером: фильтрация почты не будет остановлена, а резервная копия сервера будет защищена от попыток шифрования или вандализма.
- Запуск до окончания загрузки ОС и работа на минимально возможном уровне операционной системы не оставят злоумышленникам времени для атаки!

ОДИН КЛЮЧ для любых продуктов Dr.Web Mail Security Suite

Продукты Dr.Web для фильтрации почты Dr.Web Mail Security Suite

Unix:	MS Exchange	IBM Lotus Domino	Kerio
✓ Sendmail ✓ Postfix ✓ Exim ✓ QMail ✓ Communigate Pro ✓ Courier ✓ ZMailer			

Лицензирование

По количеству адресов	Посерверная лицензия (до 3000 адресов)	Безлимитная лицензия для любого количества серверов

Виды лицензий

- Антивирус
- Антивирус + Антиспам
- Антивирус + Антиспам + SMTP Proxy
- Антивирус + SMTP Proxy
- Антиспам + SMTP Proxy

Dr.Web совместим как с **MS Exchange**, **Lotus**, **Kerio**, так и с почтовыми серверами, работающими на платформе **Unix**, — в том числе на операционных системах, создаваемых в рамках импортозамещения.

- Подробная документация по каждому продукту.
- Круглосуточная поддержка без выходных и праздничных дней — самое быстрое решение срочных вопросов функционирования ПО Dr.Web.
- Возможность VIP-поддержки с назначением выделенного технического специалиста.
- Возможность обучения специалистов клиентов.

Трудная задача? Закажите техпресейл: по телефону, e-mail или в виде вебинара, воспользуйтесь услугой «виртуальный инженер», пригласите специалиста (Москва и область).

Dr.Web защищает по закону

- Dr.Web Mail Security Suite обладает сертификатами соответствия ФСТЭК России и ФСБ России, позволяет выполнять требования Федерального закона № 152-ФЗ «О персональных данных» в части фильтрации почтового трафика.
- Сертифицированные продукты Dr.Web могут использоваться в организациях, требующих повышенного уровня безопасности, в том числе в составе подсистемы антивирусной защиты в информационных системах персональных данных (ИСПДн) класса К1.

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 РФ.

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 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.).
- Его использование 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

Сертификаты ФСТЭК России: https://company.drweb.ru/licenses_and_certificates/fstek

Сертификаты Минобороны России: https://company.drweb.ru/licenses_and_certificates/ministry_defense

Сертификаты ФСБ России: https://company.drweb.ru/licenses_and_certificates/fsb

Все сертификаты и товарные знаки: https://company.drweb.ru/licenses_and_certificates

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
www.антивирус.рф | www.drweb.ru