Dr.WEB®
с 1992 года

Фильтрация почты антивирусами Dr.Web

Почта — самый большой источник распространения троянцев и спама

Как правило, троянцы попадают на компьютер в результате каких-либо действий пользователей — на сменных носителях или в почте.

Из обращений пользователей, пострадавших от троянца семейства Encoder, в техническую поддержку «Доктор Веб», чьи компьютеры были защищены другим антивирусом (не Dr.Web):

С почты загрузил файл — архив, после все файлы ворд и эксель а также картинки зашифрованы. Было расширение 1TXT.

Файлы зашифрованы в формате 1txt. Открыли из почты сомнительное письмо и началось шифрование.

10/10 примерно в 11 часов пришло письмо в Яндексе, открыла письмо и произошло шифрование.

Сегодня после открытия файла с почты, все файлы формата DOC, XLS превратились в файлы формата VAULT.

Добрый день! сотруднику пришло письмо от организации с архивом с пометкой срочно, он открыл, там был файл .js, после этого заразился вирусом VAULT, который зашифровал все файлы. Помогите вылечить и расшифровать данные.

Достаточно ли защиты рабочих станций, чтобы не допустить эти заражения?

Нет.

День добрый. Пришло письмо по почте с вложением "18.06.18.Gz". Открыли. Оказался вирус. На компьютере диск разбит на два логических. На диске "C" многие файлы и папки в синем цвете. На диске "D" нет.

Из обращения в техподдержку «Доктор Веб»

Анализ отчета антивируса (файла, который можно найти по адресу %userprofile%\desktop\drweb.log) показал следующую картину.

1. Шифровальщик был известен установленному на компьютере антивирусу.
2. Самое интересное заключается в том, как этот троянец запустился:

threat: DPH:Trojan.Encoder.9 ==> send user blocked alert	Запуск пользователем, антивирус идентифицирует троянца и выдает уведомление.
threat: DPH:Trojan.Encoder.9 ==> send user blocked alert	Еще один запуск!

Далее попытки запуска повторялись до тех пор, пока пользователь не решил, что раз антивирус мешает, то его лучше отключить.
И это не все причины организовать фильтрацию почты на сервере.

Почтовые потоки, проходящие через рабочую станцию и сервер, не совпадают.

- Пользователь (либо программы, на установку которых он согласился, не зная их возможностей) может отправлять и получать письма:
  - напрямую на почтовые серверы сети Интернет (по протоколу SMTP), если в сети открыт 25-й порт;
  - на почтовые службы сервисов типа mail.ru/gmail.com — по протоколам pop3/imap4.
- Пользователь (либо программы, на установку которых он согласился, не зная их возможностей) может отправлять письма по закрытым каналам, и сервер не сможет их проверить.
- Сервер (либо программы, установленные на нем) может создавать почтовые рассылки и самостоятельно уведомлять получателей и отправителей о различных событиях.

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

В описанных выше случаях пользователь просто не должен был получить зараженное письмо.

Только серверный антивирус Dr.Web для почтовых серверов в отличие от иных продуктов Dr.Web способен:

- 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;
- фильтровать почту на шлюзе, т. е. изолировав сам сервер от сети Интернет;
- проверять хранящиеся на сервере почтовые сообщения на присутствие ранее не обнаруженных угроз;
- помещать отфильтрованную почту в карантин и/или архив на случай возникновения претензий по неверной фильтрации;
- защищать все пути приема и отправки почты между почтовыми серверами филиалов компании и с внешними почтовыми сервисами (Mail.ru, Gmail и пр.);
- восстанавливать сообщения, случайно удаленные сотрудниками из почтовых ящиков, а также проводить расследования, связанные с утечкой информации.

Антивирус для фильтрации почты экономит трафик

Наличие вирусов и спама в почтовом трафике приводит к следующим проблемам:

- снижение производительности почтового сервера, занятого обработкой паразитного трафика;
- повышение нагрузки на внутреннюю сеть, снижение производительности сетевых ресурсов и пропускной способности каналов;
- выход сервера из строя в результате получения «почтовой бомбы»;
- простои оборудования.

Вирусы и спам в почтовом трафике приводят к повышению требований к аппаратной части почтовых серверов, а значит, к необходимости апгрейда или покупки новых машин.

Антивирус для фильтрации почты экономит интернет-трафик за счет возможности ограничения по приему различных вложений и возможности анализа писем при их частичном приеме.

Почту надо фильтровать комплексно

Использование антивируса без антиспама:

- 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;
- снижает производительность труда всех сотрудников компании, получающих почту и вынужденных заниматься чисткой ящиков от спама.

Антиспам Dr.Web работает на основе правил и эффективно удаляет из почтовых сообщений даже неизвестные антивирусу вредоносные программы.

Антиспам Dr.Web:

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

Преимущества антиспама Dr.Web

- Не требует обучения и начинает эффективно работать с момента установки — в отличие от антиспамов конкурентов, 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.
- Нуждается в обновлении не чаще одного раза в сутки, а значит, экономит трафик — уникальные технологии распознавания нежелательной почты на основе нескольких тысяч правил избавляют от необходимости скачивать частые и громоздкие обновления.

Продукты Dr.Web для фильтрации почты

Dr.Web Mail Security Suite

Unix: ▪ Sendmail ▪ Postfix ▪ Exim ▪ QMail ▪ Communigate Pro ▪ Courier ▪ ZMailer	MS Exchange	IBM Lotus Domino	Kerio (Windows, Linux, macOS)

Возможности управления:

- **Управление через веб-интерфейс.**
- **Управление через консоль Dr.Web Enterprise Suite.** Интеграция в систему Dr.Web Enterprise Suite позволяет обеспечить управление системой антивирусной защиты «из одной точки» с максимальным удобством для системного администратора.
- **Управление через утилиты командной строки.**

ОДИН КЛЮЧ для любых продуктов Dr.Web Mail Security Suite.

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

! Максимальное качество фильтрации достигается при использовании почтового шлюза **Dr.Web SMTP proxy** — фильтра, обрабатывающего сообщения до их попадания на почтовый сервер.
Не нужно получать никакого вредоносного письма, если у вас сервер выставлен в Интернет, — атакующий сам вас найдет (например, перебором адресов).
Использование **Dr.Web SMTP proxy:**

- существенно повышает общую безопасность сети;
- значительно улучшает качество фильтрации за счет отсутствия ограничений, накладываемых почтовыми серверами;
- снижает нагрузку на внутренние почтовые серверы и рабочие станции;
- повышает стабильность работы системы проверки почты в целом.

Использование демилитаризованной зоны и средств проверки почтового трафика на уровне SMTP-шлюза повышает уровень защиты.

Почтовый сервер тоже должен быть защищен

Почтовый сервер — это просто сервис, размещающийся на обычном файловом сервере. Поэтому кроме защиты почтового сервиса необходимо использовать и защиту самого сервера и каналов коммуникаций с ним.

- Почтовый сервер может быть заражен как изнутри, так и снаружи.
- 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
▪ Снижение производительности сервера или его полная неработоспособность (простои). ▪ Повышение нагрузки на внутреннюю сеть, снижение производительности сетевых ресурсов и пропускной способности каналов. ▪ Отказ в обслуживании — отключение предприятия от сети Интернет или внесение в черные списки за рассылку спама в случае попадания в бот-сеть. ▪ 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 сотрудниками должностных обязанностей; – задержки в выполнении обязательств компании перед клиентами; – блокирование получения почты партнерами за счет внесения компании в черные списки; ▪ ухудшение репутации в глазах потребителей и партнеров; ▪ мнение о компании как о технологически отсталой; ▪ уход клиентов — отказ от услуг компании.

Антивирус для защиты сервера экономит трафик

- 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!

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

- Имеющиеся в составе Dr.Web Server Security Suite для Windows технологии превентивной защиты защитят даже от еще не известных угроз и эксплойтов, попыток коммуникаций удаленно управляемых вредоносных объектов с сервером злоумышленников (для управления ботнетами и шпионажа). Без зависимости от вирусных баз и частоты их обновлений.
- 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!** Работа на минимально возможном уровне операционной системы!

О компании «Доктор Веб»

«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.

«Доктор Веб» стал первой компанией, предложившей на российском рынке инновационную модель использования антивируса в качестве услуги, и по сей день продолжает оставаться безусловным лидером российского рынка интернет-сервисов безопасности для поставщиков ИТ-услуг.

Dr.Web доверяют

Наличие в штате «Доктор Веб» экспертов по различным вопросам информационной безопасности позволяет компании максимально учитывать особенности работы предприятий самого разного размера и профиля деятельности и предлагать клиентам оптимальный выбор качественных продуктов, имеющих минимальную совокупную стоимость.

Среди потребителей продуктов компании — домашние пользователи из всех регионов мира и крупные российские предприятия, небольшие организации и системообразующие корпорации. География пользователей Dr.Web свидетельствует о высоком доверии к продукту, созданному талантливыми программистами России.

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

Почему Dr.Web?

Все права на технологии Dr.Web принадлежат компании «Доктор Веб». Компания является одним 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.

Адреса:

РОССИЯ
ООО «Доктор Веб»
125124, Москва, 3-я улица Ямского поля, вл. 2, корп.12 а
Телефон: +7 (495) 789-45-87 (многоканальный)
Факс: +7 (495) 789-45-97
Бесплатный телефон технической поддержки:
8-800-333-7932
www.drweb.ru | curenet.drweb.ru | www.av-desk.com | free.drweb.ru

ГЕРМАНИЯ
Doctor Web Deutschland GmbH
Rodenbacher Chaussee 6, D-63457 Hanau
Телефон: +49 (6039) 939-5414
Факс: +49 (6039) 939-5415
www.drweb-av.de

КАЗАХСТАН
ТОО «Доктор Веб – Центральная Азия»
050009, Алматы, ул. Шевченко / уг. ул. Радостовца,
165б/72г, офис 910
Телефон: +7 (727) 323-62-30, 323-62-31, 323-62-32
www.drweb.kz

КИТАЙ
Doctor Web Software Company (Tianjin), Ltd.
Тяньцзинская зона экономического и технического
развития, 4 проспект, д. 80, технопарк «Тяньда»,
северный софт-корпус
天津市经济技术开发区第四大街80号软件大厦北楼112
Телефон: +86-022-59823480
Факс: +86-022-59823480
E-mail: y.zhang@drweb.com
www.drweb.cn

УКРАИНА
ООО «Центр технической поддержки «Доктор Веб»
01601, Украина, г. Киев, ул. Пушкинская, д. 27,
5-й этаж, оф. 6
Телефон/факс: +38 (044) 238-24-35, 279-77-70
www.drweb.ua

ФРАНЦИЯ
Doctor Web France
333 b Avenue de Colmar, 67100 STRASBOURG
Телефон: +33 (0) 3-90-40-40-20
Факс: +33 (0) 3-90-40-40-21
www.drweb.fr

ЯПОНИЯ
Doctor Web Pacific, Inc.
NKF Kawasaki building 2F, 1-2, Higashida-cho, Kawasaki-ku,
Kawasaki-shi, Kanagawa-ken
210-0005, Japan
Телефон: +81 (0) 44-201-7711
www.drweb.co.jp

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