Dr.WEB®
始创于1992年

使用Dr.Web反病毒产品进行邮件过滤

邮箱是木马和垃圾邮件最大的传播源。

通常木马是由于用户使用移动载体或邮箱时采取的某些操作才得以入侵电脑

以下内容摘选自Encoder家族木马受害者向Doctor Web公司技术支持部门的求助申请，其电脑使用的是其他厂商的反病毒产品（而非Dr.Web产品）：

我从邮箱下载了一个文件：是压缩文件，随后所有Word和Excel的文件和图片就都被加了密。加密后文件的扩展名为1TXT。

文件被加密后的格式是1txt。**我在邮箱中打开了**一个可疑邮件，之后电脑上的文件就被加密了。

10月10号11点左右我的Yandex邮箱收**到一封邮件**，我打开邮件后电脑上的文件就被加密了。

今天在邮箱打开了一个文件，之后电脑上所有DOC、XLS的文件就都变成了VAULT格式文件。

您好!我公司员工收到一封来自企业、标为紧急的邮件，邮件还带有压缩文件附件，打开后发现.js文件，随后感染了VAULT病毒，所有文件均被加密。请帮助我们清除病毒并对数据解密。

对工作站实施的保护是否足以防止此类感染?

对此的回答是“否”。

您好。我收到一封带有附件“18.06.18.Gz”的邮件，打开了，结果这是个病毒。计算机有两个逻辑盘，C盘的文件和文件夹变成了蓝色，D盘没有。

摘自Doctor Web公司技术支持部门收到的求助

对反病毒报告作出的分析（此报告的位置是%userprofile%\desktop\drweb.log地址找到的

地址找到的文件）显示:

1. 这个加密木马对于安装在电脑的反病毒软件而言是一个移至威胁。
2. 最有意思的是这一木马是怎么启动的：

threat: DPH:Trojan.Encoder.9 ==> send user blocked alert	用户启动了木马，反病毒软件识别了木马并发出通知。
threat: DPH:Trojan.Encoder.9 ==> send user blocked alert	再次启动！

随后木马会重复启动，直到用户决定是反病毒程序出现了问题，在妨碍操作，所以停用了反病毒软件。

这还不是需要在服务器进行邮件过滤的全部原因。

通过工作站和服务器的邮件流并不是同一个邮件流。

- 用户（或者是用户在不清楚其功能的情况下安装的程序）可以发送或收取邮件:
  - 用户（或者是用户在不清楚其功能的情况下安装的程序）可以发送或收取邮件;
  - 使用协议pop3/imap4发送到mail.ru/gmail.com邮箱服务.
- 用户（或者是用户在不清楚其功能的情况下安装的程序）能够使用秘密管道发送邮件，服务器无法对其进行检查。
- 服务器（或安装在服务器上的程序）可以创建邮件群发并自行向收件人和发件人发送不同事件的通知。

通过邮箱进入公司或从公司出去的所有信息都应在到达用户计算机和设备前进行检查。

这样用户才不会收到被感染的邮件。

只有用于邮件服务器Dr.Web服务器保护产品能够

- 在公司自己的服务器或租用服务器过滤外部（传入和传出）邮件和公司内部邮件，查找病毒和垃圾邮件；
- 在网关过滤邮件，也就是将服务器与互联网网络隔离；
- 检查保存在服务器上的邮件是否存在之前未发现的威胁；
- 将过滤后的邮件移至隔离区和/或存档，如果出现认为过滤出错的情况，可以进行分析；
- 保护公司分支机构的邮件服务器至今以及与外部邮件服务（Mail.ru，Gmail等）之间接收和发送邮件的所有通道；
- 能够还原员工从邮箱中意外删除的邮件，还可以协作调查信息泄漏事件。

反病毒产品过滤邮箱可节省流量

邮件流量中存在病毒和垃圾邮件会导致:

- 邮件服务器因处理寄生流量而降低性能；
- 增加内部网络的负载，降低网络资源和带宽信道的性能；
- 因接收“邮件炸弹”而导致服务器故障；
- 设备停滞。

邮箱流量存在病毒和垃圾邮件会提高对邮件服务器硬件的要求，也就是需要进行设备升级或购买新机器。

进行邮箱过滤的反病毒产品可以限制接收各种附件，并在部分接收时就进行分析，因此能够节省互联网流量。

需要对邮件进行综合过滤

需要对邮件进行综合过滤:

- 会导致黑客有机会对公司的邮件服务器和员工的邮件客户端进行网络钓鱼攻击；在某些情况下，只是收到一封邮件就足以让机器被感染或性能遭到破坏；
- 导致流量费用增多；
- 导致邮件服务器上寄生负载增加；
- 接收和处理垃圾邮件会降低公司所有员工的工作效率。

Dr.Web反垃圾邮件使用过滤规则，有效删除电子邮件中含有的恶意程序，包括反病毒软件未知的恶意程序。

Dr.Web反垃圾邮件:

- 作为解决方案的组成部分，不以单独产品的形式提供
- 同过滤病毒的产品同时安装到同一个服务器。

这样可以简化管理，保证总价比同类产品更低。

Dr.Web反垃圾邮件的优势

- 无需进行培训，安装后即开始有效运行，优于使用贝叶斯算法的反垃圾邮件。
- 对垃圾邮件的判断不取决于邮件使用的语言。
- 可对不同类型的垃圾邮件设置不同的处理操作。
- 使用自身的黑白名单防止将公司恶意加入黑名单而造成损害。
- 误报极少。
- 一日最多更新一次，这样可以节省流量。使用几千条规则侦测不需要的邮件，因此没有必要经常更新。

用于过滤邮件的Dr.Web产品

Dr.Web Mail Security Suite

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

管理功能

- 通过Web界面进行管理
- 通过Dr.Web Enterprise Suite控制台进行管理。与Dr.Web Enterprise Suite系统一体化可以 “从一个点” 管理反病毒保护系统，为系统管理员提供极大便利。
- 通过命令行工具进行管理。

所有Dr.Web Mail Security Suite产品使用的是同一个密钥

授权

按照地址数量	服务器授权（不超过3000个地址）	服务器授权（不超过3000个地址）

授权形式

- 反病毒
- 反病毒 + 反垃圾邮件
- 反病毒 + 反垃圾邮件 + SMTP Proxy
- 反病毒 + SMTP Proxy
- 反垃圾邮件 + SMTP Proxy

! 使用Dr.Web SMTP proxy邮件网关时，是在邮件到达邮件服务器前进行过滤，可实现最高质量的过滤。如果您的服务器连接互联网，则在没有接收任何恶意邮件也会受害，因为攻击者会自己找上门来（比如，利用穷举搜索地址）

使用Dr.Web SMTP proxy：

- 可从总体上大大提高网络的安全性；
- 没有邮件服务器所设置的限制，可大大提升过滤质量；
- 降低内部邮件服务器和工作站的负载；
- 提高邮件检查系统的整体运行稳定性。

在SMTP网关级别使用网络外围和邮件流量检查工具可提高保护级别。

邮件服务器同样也需要保护

邮件服务器只是一个置于普通文件服务器的服务，所以除了保护邮箱服务，还需要保护服务器本身和与之联系的通道。

- 邮件服务器可能是从内网被感染，也可能是从外网被感染。
- 只有保护服务器本身以及与之联系的通道（包括内网和外网）才能避免在未知病毒入侵网络时成为感染源。
- 所有位于公司内部或在外部租用的服务器都需要被保护。

服务器被感染导致的技术性负面影响	服务器被感染导致的商业影响
▪ 降低服务器性能或使其完全无法运行（死机）。 ▪ 增加内部网络的负载，降低网络资源和带宽信道的性能。 ▪ 服务中断，企业断网或在落入僵尸网络时被列入垃圾邮件群发黑名单。 ▪ 增加IT基础架构成本（支付过量流量 / 增加服务器数量 / 保存包括垃圾邮件在内的邮件的费用）。	▪ 破坏企业流程的连续性: – 耽误员工执行工作职责； – 耽误员工对客户通过服务； – 由于公司被列入黑名单而使合作伙伴无法接收邮件； ▪ 影响消费者和合作伙伴对公司的评价； ▪ 公司会被认为是技术落后的公司； ▪ 客户拒绝公司提供的服务，造成客户流失

保护服务器的反病毒产品可节省流量

- 邮件仅在服务器过滤一次，而不是在每个工作站过滤多次。这样可提高运行速度，大大减少员工对计算机速度缓慢的抱怨。
- 由于Dr.Web产品采用加密和压缩算法，可大幅减少内部网络的流量，其他厂商工作站保护产品不具备此功能。
- 使用Dr.Web Mail Security Suite反垃圾邮件后，邮件服务器的寄生负载会降低（垃圾邮件在邮件流量中高达98%，将其筛除可提高邮件服务器的运行能力）。邮件接收延迟和信件丢失的情况将极少发生！

您的正确选择：Dr.Web Server Security Suite + Dr.Web Mail Security Suite

- Dr.Web Server Security Suite for Windows包含的预防性保护技术可以抵御未知威胁和漏洞攻击代码，阻止不法分子控制的恶意对象与其服务器（用于管理僵尸网络和间谍活动）进行远程连接。不依赖于病毒库和更新频率。
- Dr.Web SelfPROtect自我保护模块在市场上没有同类产品，能够防止Dr.Web反病毒产品出现故障，阻止不法分子获取服务器管理权限，不会停止过滤邮件，服务器备份将避免被加密或破坏。
- 在操作系统加载结束前启动！在操作系统最低级别运行!

关于Doctor Web公司

Doctor Web公司是俄罗斯信息安全反病毒保护产品厂商，产品商标为Dr.Web。1992年开始研发Dr.Web反病毒软件，在俄罗斯信息安全软件市场占据重要位置。

Doctor Web公司是俄罗斯市场上首家提供反病毒产品服务创新模式的公司，对于俄罗斯IT服务供应商来说，Doctor Web公司至今仍是俄罗斯互联网安全服务市场上无可争议的领军企业。

客户信赖Dr.Web产品的

Doctor Web公司技术力量雄厚，拥有各类信息安全问题专家，能够充分考虑不同规模、不同行业企业运行特点，为客户提供最佳性价比产品。

公司产品用户包括分布全球的个人用户、大型企业、中小型单位以及行业支柱性集团公司。Dr.Web用户之广是对俄罗斯卓越软件研发产品无比信任的见证。

这里列出的仅是Dr.Web产品的部分客户：https：//customers.drweb.com。

为什么选择Dr.Web?

Dr.Web技术的所有权利属于DoctorWeb公司。Doctor Web公司是世界上为数不多的拥有自主研发的独有恶意软件侦测技术和清除技术的公司之一。公司设有自己的反病毒研究室、全球病毒监控部和技术支持部。

天津市经济技术开发区第四大街80
号软件大厦北楼112
联系电话: +86-022-59823480
传真: +86-022-59823480
E-mail: y.zhang@drweb.com
www.drweb.cnhttps://www.drweb.cn