(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 105991395 B
(45)授权公告日 2019.04.09

(21)申请号 201510051147.8

(22)申请日 2015.01.30

(65)同一申请的已公布的文献号
申请公布号 CN 105991395 A

(43)申请公布日 2016.10.05

(73)专利权人 杭州迪普科技股份有限公司
地址 310051 浙江省杭州市滨江区通和路68号中财大厦6层

(72)发明人 张园慕野

(74)专利代理机构 北京博思佳知识产权代理有限公司 11415
代理人 林祥

(51)Int.Cl.
H04L 12/58(2006.01)

(56)对比文件
CN 101079689 A,2007.11.28,
CN 101789105 A,2010.07.28,
US 2003097409 A1,2003.05.22,
CN 103546449 A,2014.01.29,
CN 1863221 A,2006.11.15,

审查员 章鹏

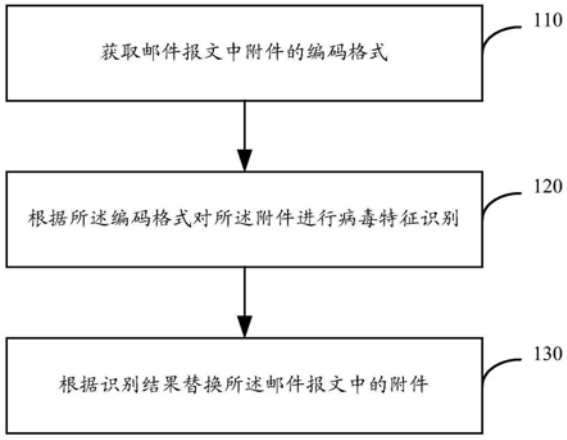
权利要求书2页 说明书4页 附图2页

(54)发明名称

附件替换方法及装置

(57)摘要

本申请提供一种附件替换方法及装置,应用于网络设备上,该方法包括:获取邮件报文中附件的编码格式;根据所述编码格式对所述附件进行病毒特征识别;根据识别结果替换所述邮件报文中的附件。通过本申请可以更加准确识别病毒附件,从而彻底清除病毒附件,提高对病毒附件的处理效率,真正达到防病毒效果。



CN 105991395 B

1.一种附件替换方法,应用于网络设备上,其特征在于,该方法包括:

获取邮件报文中附件的编码格式;

判断所述编码格式是否属于加密格式;

根据判断结果对所述附件进行病毒特征识别;

根据识别结果替换所述邮件报文中的附件。

2.如权利要求1所述的方法,其特征在于,所述根据判断结果对所述附件进行病毒特征识别,包括:

当所述编码格式属于加密格式时,根据所述编码格式对所述附件进行解码;对解码后的附件进行病毒特征识别;

当所述编码格式不属于加密格式时,对所述附件进行病毒特征识别。

3.如权利要求1所述的方法,其特征在于,所述判断所述编码格式是否属于加密格式,包括:

对所述附件进行病毒特征识别;

当识别结果为所述附件未携带病毒特征时,判断所述编码格式是否属于加密格式;

所述根据判断结果对所述附件进行病毒特征识别,包括:

当所述编码格式属于加密格式时,根据所述编码格式对所述附件进行解码;对解码后的附件进行病毒特征识别。

4.如权利要求1所述的方法,其特征在于,所述获取邮件报文中附件的编码格式之前,还包括:

配置所述邮件报文的入接口;

在所述入接口上配置防病毒策略;

所述根据识别结果替换所述邮件报文中的附件,包括:

当所述识别结果为所述附件携带病毒特征时,判断所述邮件报文是否为从所述入接口接收的报文;

当所述邮件报文为从所述入接口接收的报文时,判断所述入接口上配置的防病毒策略是否为病毒替换策略;

当所述入接口上的防病毒策略为所述病毒替换策略时,替换所述邮件报文中的附件。

5.如权利要求4所述的方法,其特征在于,所述替换所述邮件报文中的附件,包括:

当所述附件的编码格式属于加密格式时,获取所述附件在邮件报文中的位置信息;根据所述附件的位置信息替换整个附件;

当所述附件的编码格式不属于加密格式时,获取所述附件中病毒代码的位置信息;替换所述附件中的病毒代码。

6.一种附件替换装置,应用于网络设备上,其特征在于,该装置包括:

获取单元,用于获取邮件报文中附件的编码格式;

识别单元,用于判断所述编码格式是否属于加密格式;根据判断结果对所述附件进行病毒特征识别;

替换单元,用于根据识别结果替换所述邮件报文中的附件。

7.如权利要求6所述的装置,其特征在于:

所述识别单元,具体用于当所述编码格式属于加密格式时,根据所述编码格式对所述

附件进行解码;对解码后的附件进行病毒特征识别;当所述编码格式不属于加密格式时,对所述附件进行病毒特征识别。

8.如权利要求6所述的装置,其特征在于:

所述识别单元,具体用于对所述附件进行病毒特征识别;当识别结果为所述附件未携带病毒特征时,判断所述编码格式是否属于加密格式;当所述编码格式属于加密格式时,根据所述编码格式对所述附件进行解码;对解码后的附件进行病毒特征识别。

9.如权利要求6所述的装置,其特征在于,所述装置还包括:

配置单元,用于在所述获取单元获取邮件报文中附件的编码格式之前,配置所述邮件报文的入接口;在所述入接口上配置防病毒策略;

所述替换单元,具体包括:

接口判断模块,用于当所述识别结果为所述附件携带病毒特征时,判断所述邮件报文是否为从所述入接口接收的报文;

策略判断模块,用于当所述邮件报文为从所述入接口接收的报文时,判断所述入接口上配置的防病毒策略是否为病毒替换策略;

附件替换模块,用于当所述入接口上的防病毒策略为所述病毒替换策略时,替换所述邮件报文中的附件。

10.如权利要求9所述的装置,其特征在于:

所述附件替换模块,具体用于当所述附件的编码格式属于加密格式时,获取所述附件在邮件报文中的位置信息;根据所述附件的位置信息替换整个附件;当所述附件的编码格式不属于加密格式时,获取所述附件中病毒代码的位置信息;替换所述附件中的病毒代码。

附件替换方法及装置

技术领域

[0001] 本申请涉及网络通信技术领域，尤其涉及附件替换方法及装置。

背景技术

[0002] 电子邮件是一种重要的信息交换方式，尤其在办公应用中。由于网络安全形势严峻，电子邮件容易受到邮件病毒的恶意攻击。邮件病毒主要携带在附件中，当用户浏览或下载附件时造成用户主机感染病毒，进而破坏主机的系统以及文件等，造成信息丢失等严重后果。目前，对病毒附件的识别和处理不够彻底，处理效率低，且效果不佳。

发明内容

[0003] 有鉴于此，本申请提供了一种附件替换方法，应用于网络设备上，该方法包括：

[0004] 获取邮件报文中附件的编码格式；

[0005] 根据所述编码格式对所述附件进行病毒特征识别；

[0006] 根据识别结果替换所述邮件报文中的附件。

[0007] 本申请还提供了一种附件替换装置，应用于网络设备上，该装置包括：

[0008] 获取单元，用于获取邮件报文中附件的编码格式；

[0009] 识别单元，用于根据所述编码格式对所述附件进行病毒特征识别；

[0010] 替换单元，用于根据识别结果替换所述邮件报文中的附件。

[0011] 本申请针对不同编码格式的附件采取不同的病毒识别方法，并在识别出病毒后，对病毒附件进行替换。通过本申请可以更加准确识别病毒附件，从而彻底清除病毒附件，提高对病毒附件的处理效率，真正达到防病毒效果。

附图说明

[0012] 图1是本申请一种实施例中附件替换方法的处理流程图；

[0013] 图2是本申请一种实施例中附件替换装置的基础硬件示意图；

[0014] 图3是本申请一种实施例中附件替换装置的结构示意图。

具体实施方式

[0015] 为使本申请的目的、技术方案及优点更加清楚明白，以下参照附图对本申请所述方案作进一步地详细说明。

[0016] 电子邮件是互联网中应用最广泛的一种通信方式，可以承载大量用户希望获得的信息，且通常采用附件的形式携带在电子邮件中。由于网络安全形势日益严峻，电子邮件很容易受到病毒的恶意攻击，且大量病毒主要携带在附件中。当用户浏览或下载附件时，病毒会潜伏到用户主机上，当病毒发作时，破坏用户主机系统以及文件等，影响主机的正常使用，甚至造成重要信息丢失等严重后果。目前，针对病毒附件的识别和处理都不够彻底，处理效率低，且效果不佳。

[0017] 针对上述问题，本申请实施例提出一种附件替换方法，该方法根据附件的编码格式采取相应的病毒识别方法，并在识别出病毒附件后，对病毒附件进行替换。

[0018] 参见图1，为本申请附件替换方法的一个实施例流程图，该实施例对附件替换的处理过程进行描述。

[0019] 步骤110，获取邮件报文中附件的编码格式。

[0020] 在对电子邮件进行防病毒控制之前，网络管理员可以根据实际的控制需求在网络设备上进行防病毒配置，具体包括：配置邮件报文的入接口，以及在该入接口上拟采取的防病毒策略。其中，邮件报文为承载电子邮件的报文，目前，比较流行的邮件报文包括SMTP(Simple Mail Transfer Protocol，简单邮件传输协议)、POP3(Post Office Protocol-Version，邮局协议版本3)以及IMAP4(Internet Message Access Protocol 4，交互式数据消息访问协议第四个版本)；入接口为网络设备接收电子邮件的接口。在某一接口上配置的防病毒策略只适用于当前接口，其中，防病毒策略可以为病毒替换、病毒删除等，可根据实际控制需求进行配置。本申请实施例中，将防病毒策略配置为病毒替换，即在识别出携带病毒的附件时，替换掉病毒附件，从而起到防病毒的作用。

[0021] 在完成上述配置后，网络设备开始接收报文进行处理。首先，需要对接收的报文进行协议识别，例如，可以通过固定端口号、报文特征匹配等现有的识别方式判断接收的报文是否为邮件报文。在确定为邮件报文时，从报文头中获取附件配置信息，该附件配置信息表明该邮件报文中是否存在附件。当存在附件时，从报文头中获取附件的编码格式，目前，已知的附件编码格式包括7bit(7位编码)、8bit(8位编码)、binary(二进制编码)、quoted-printable(可打印字符引用编码)、base64(基础64编码)以及custom(定制编码)，其中，常用的编码格式为7bit、quoted-printable以及base64。通过上述编码格式将附件转化成ASCII(American Standard Code for Information Interchange，美国信息互换标准代码)码格式，这是由于电子邮件只能传输ASCII格式的信息。

[0022] 步骤120，根据所述编码格式对所述附件进行病毒特征识别。

[0023] 步骤110提到的几种编码格式可以分为两大类：加密格式和明文格式，例如，quoted-printable和base64属于加密格式，7bit属于明文格式。

[0024] 在一种实施方式中，网络设备获取到附件的编码格式后，首先判断该编码格式是否属于加密格式，根据判断结果进行如下处理：

[0025] 如果附件的编码格式属于加密格式，则根据具体编码格式对附件进行解码，例如，附件编码格式为quoted-printable时，则根据该quoted-printable编码格式的特征进行解码，解码后进行病毒特征识别。

[0026] 如果附件的编码格式不属于加密格式，即附件的编码格式属于明文格式，则可以直接对附件进行病毒特征识别。

[0027] 在对上述处理后的附件进行病毒特征识别时，可以通过病毒特征引擎在附件中查找病毒特征，其中，该病毒特征引擎是根据已搜集到所有病毒特征编译的引擎。当在附件中找到病毒特征时，记录对应病毒代码在邮件报文中的位置信息，包括起始位置和结束位置。

[0028] 在另一种实施方式中，网络设备接收邮件报文后，直接利用病毒特征引擎对附件进行病毒特征识别。如果识别出病毒特征，说明附件的编码格式属于明文格式，记录对应病毒代码在邮件报文中的起始位置和结束位置；当未识别出病毒特征时，说明附件中可能没

有病毒或者附件的编码格式可能属于加密格式，此时，判断附件的编码格式是否属于加密格式，如果属于加密格式，则根据编码格式对附件解码，解码后进行病毒特征识别。

[0029] 步骤130，根据识别结果替换所述邮件报文中的附件。

[0030] 在经过步骤120的病毒特征识别后，如果识别的结果为附件携带病毒特征，则判断携带该附件的邮件报文是否为从预先配置的入接口接收的报文，当该邮件报文为从预先配置的入接口接收的报文时，进一步判断该入接口上配置的防病毒策略是否为病毒替换策略，在确认为病毒替换策略时，替换该邮件报文中的附件。

[0031] 在进行附件替换时，根据附件的编码格式不同，其附件替换方式也不同。首先，判断附件的编码格式是否属于加密格式，根据判断结果进行如下处理：

[0032] 当附件的编码格式属于加密格式时，获取该附件在邮件报文中的位置信息，该位置信息包括起始位置和结束位置，其中，附件的位置信息可通过MIME(Multipurpose Internet Mail Extensions，多用途互联网邮件扩展类型)解析器在附件解码前获取。由于对加密格式的附件解码再编码需要较大的缓存，且占用大量的CPU处理时间，因此，对于加密格式的附件一旦发现病毒特征即根据获得的附件位置信息替换整个附件，以提高防病毒的处理效率。

[0033] 当附件的编码格式不属于加密格式时，获取附件中病毒代码的位置信息，例如，如前所述，病毒代码的位置信息可在通过病毒特征引擎对附件进行病毒识别时获得。对于非加密格式的附件只针对病毒代码部分进行替换，以保证附件的部分有效。

[0034] 此外，在前述识别出附件中的病毒特征时，可以在病毒告警日志中记录该病毒特征的标识，向日志服务器发送该病毒告警日志，以便网络管理员及时掌握系统中邮件受攻击情况，根据病毒特征采取有针对性的防御措施。

[0035] 与前述附件替换方法的实施例相对应，本申请还提供附件替换装置的实施例。

[0036] 本申请附件替换装置的实施例可以应用在网络设备上。装置实施例可以通过软件实现，也可以通过硬件或者软硬件结合的方式实现。以软件实现为例，作为一个逻辑意义上的装置，是通过其所在设备的CPU运行存储器中对应的计算机程序指令形成的。从硬件层面而言，如图2所示，为本申请附件替换装置所在设备的一种硬件结构图，除了图2所示的CPU、存储器之外，实施例中装置所在的设备通常还可以包括其他硬件。

[0037] 请参考图3，为本申请一个实施例中的附件替换装置的结构示意图。该附件替换装置包括获取单元301、识别单元302以及替换单元303，其中：

[0038] 获取单元301，用于获取邮件报文中附件的编码格式；

[0039] 识别单元302，用于根据所述编码格式对所述附件进行病毒特征识别；

[0040] 替换单元303，用于根据识别结果替换所述邮件报文中的附件。

[0041] 进一步地，

[0042] 所述识别单元302，具体用于判断所述编码格式是否属于加密格式；当所述编码格式属于加密格式时，根据所述编码格式对所述附件进行解码；对解码后的附件进行病毒特征识别；当所述编码格式不属于加密格式时，对所述附件进行病毒特征识别。

[0043] 进一步地，

[0044] 所述识别单元302，具体用于对所述附件进行病毒特征识别；当识别结果为所述附件未携带病毒特征时，判断所述编码格式是否属于加密格式；当所述编码格式属于加密格

式时，根据所述编码格式对所述附件进行解码；对解码后的附件进行病毒特征识别。

[0045] 进一步地，所述附件替换装置还包括：

[0046] 配置单元，用于在所述获取单元获取邮件报文中附件的编码格式之前，配置所述邮件报文的入接口；在所述入接口上配置防病毒策略；

[0047] 所述替换单元303，具体包括：

[0048] 接口判断模块，用于当所述识别结果为所述附件携带病毒特征时，判断所述邮件报文是否为从所述入接口接收的报文；

[0049] 策略判断模块，用于当所述邮件报文为从所述入接口接收的报文时，判断所述入接口上配置的防病毒策略是否为病毒替换策略；

[0050] 附件替换模块，用于当所述入接口上的防病毒策略为所述病毒替换策略时，替换所述邮件报文中的附件。

[0051] 进一步地，

[0052] 所述附件替换模块，具体用于判断所述附件的编码格式是否属于加密格式；当所述附件的编码格式属于加密格式时，获取所述附件在邮件报文中的位置信息；根据所述附件的位置信息替换整个附件；当所述附件的编码格式不属于加密格式时，获取所述附件中病毒代码的位置信息；替换所述附件中的病毒代码。

[0053] 上述图3示出的附件替换装置的实施例，其具体实现过程可参见前述方法实施例的说明，在此不再赘述。

[0054] 从以上方法和装置的实施例中可以看出，本申请针对不同编码格式的附件采取不同的病毒识别方法，并在识别出病毒后，对病毒附件进行替换。通过本申请可以更加准确识别病毒附件，从而彻底清除病毒附件，提高对病毒附件的处理效率，真正达到防病毒效果。

[0055] 以上所述仅为本申请的较佳实施例而已，并不用以限制本申请，凡在本申请的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本申请保护的范围之内。

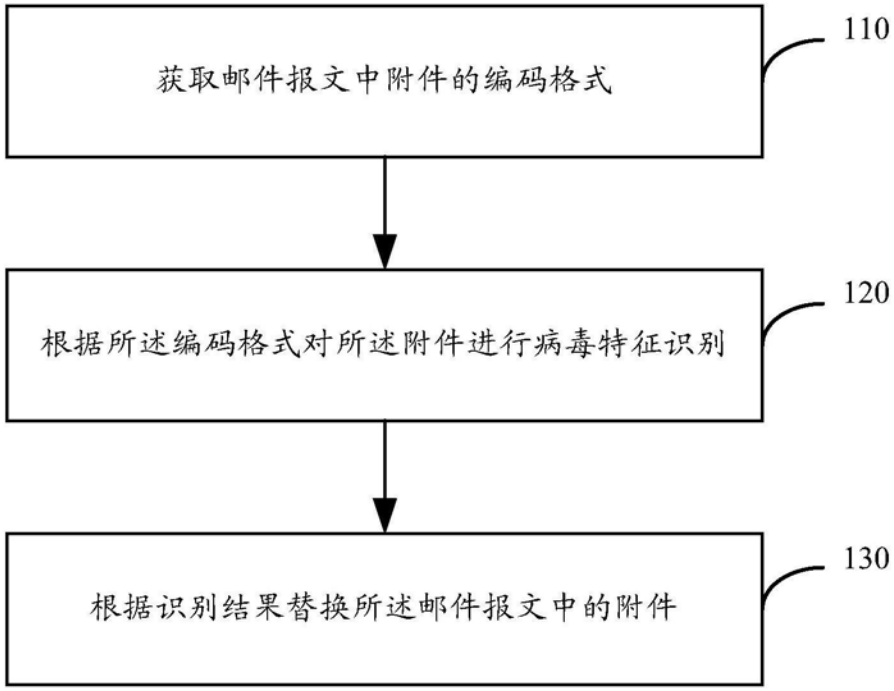

获取邮件报文中附件的编码格式
110
根据所述编码格式对所述附件进行病毒特征识别
120
根据识别结果替换所述邮件报文中的附件
130

图1

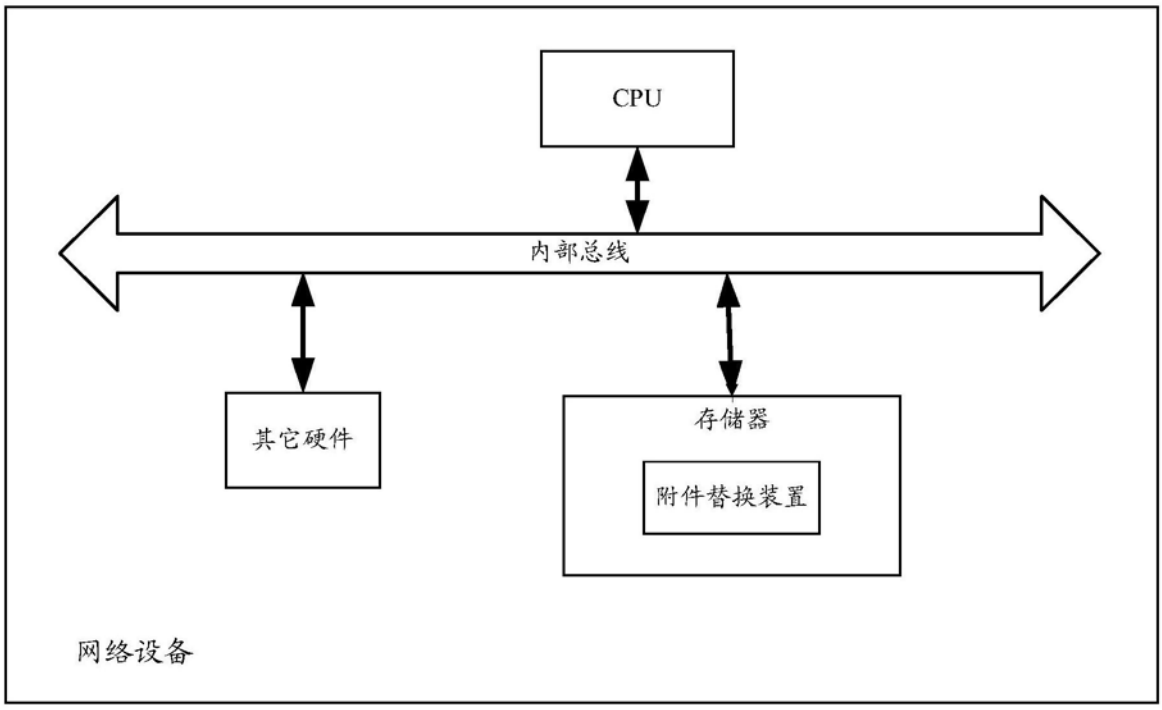

CPU
内部总线
其它硬件
存储器
附件替换装置
网络设备

图2

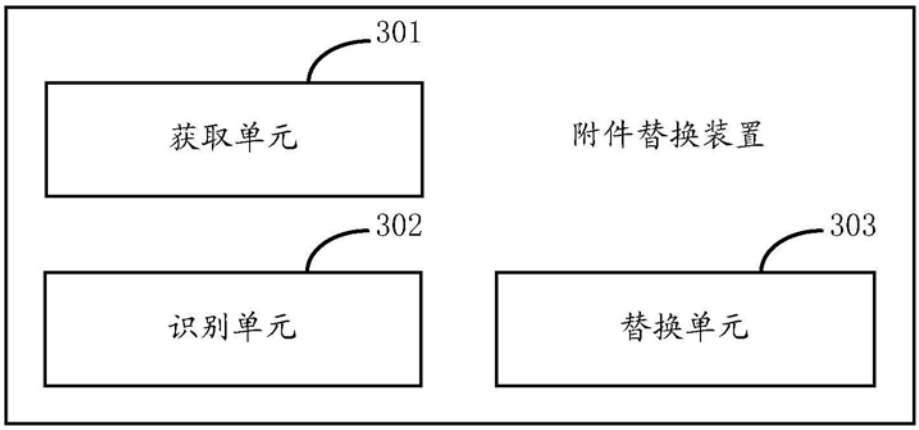


图3