(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 116204880 A
(43)申请公布日 2023.06.02

(21)申请号 202211738230.9

(22)申请日 2022.12.30

(71)申请人 重庆信锐达科技有限公司
地址 401121 重庆市渝北区黄山大道中段杨柳路3号2幢20层2001号

(72)发明人 方少林

(74)专利代理机构 重庆仟佰度专利代理事务所(普通合伙) 50295
专利代理师 廖龙春

(51)Int.Cl.
G06F 21/56(2013.01)
G06F 21/53(2013.01)

权利要求书1页 说明书4页 附图1页

(54)发明名称

一种计算机病毒防御系统

(57)摘要

本发明涉及计算机技术领域，具体公开了一种计算机病毒防御系统，包括：用户画像模块，用于记录用户的计算机操作行为，分析用户的计算机熟悉程度，基于预设的分类规则和计算机熟悉程度确定用户的分类；用户的分类包括低风险用户、中风险用户和高风险用户；等级确定模块，用于根据用户的分类确定当前的防护等级；在防护等级为高时，启用邮件防护模式；在防护等级为低时，关闭邮件防护模块；邮件防护模块，用于在启用邮件防护模式后，判断新接收的电子邮件中是否包含附件，如果包含附件，将附件发送至沙盒中，在沙盒中对附件进行分析，判断附件中是否包含勒索病毒，如果包含勒索病毒，生成报警信息。采用本发明的技术方案能够有效减少系统资源占用。

CN 116204880 A

1.一种计算机病毒防御系统,其特征在于,包括:

用户画像模块,用于记录用户的计算机操作行为,根据计算机操作行为分析用户的计算机熟悉程度,基于预设的分类规则和计算机熟悉程度确定用户的分类;用户的分类包括低风险用户、中风险用户和高风险用户;

等级确定模块,用于根据用户的分类确定当前的防护等级;在防护等级为高时,启用邮件防护模式;在防护等级为低时,关闭邮件防护模块;

邮件防护模块,用于在启用邮件防护模式后,判断新接收的电子邮件中是否包含附件,如果包含附件,将附件发送至沙盒中,在沙盒中对附件进行分析,判断附件中是否包含勒索病毒,如果包含勒索病毒,生成报警信息。

2.根据权利要求1所述的计算机病毒防御系统,其特征在于:所述用户画像模块还用于获取计算机存储设备上的文件列表,根据文件列表分析数据重要等级,基于预设的分类规则、计算机熟悉程度和数据重要等级确定用户的分类。

3.根据权利要求2所述的计算机病毒防御系统,其特征在于:所述用户画面模块还用于记录计算机状态信息,基于预设的分类规则、计算机熟悉程度、据重要等级和计算机状态信息确定用户的分类;计算机状态信息包括计算机操作系统信息、软件安装信息和硬件信息。

4.根据权利要求3所述的计算机病毒防御系统,其特征在于:所述等级确定模块还用于未确定当前的防护等级前,将初始防护等级设置为高;

等级确定模块还用于根据用户的分类生成防护等级建议信息;根据获取的用户的防护等级选择信息确定当前的防护等级;其中防护等级建议信息包括建议低防护等级、建议中防护等级或建议高防护等级。

5.根据权利要求4所述的计算机病毒防御系统,其特征在于:所述等级确定模块还用于在防护等级为中时,启用邮件防护模式;

邮件防护模块还用于在启用邮件防护模式且防护等级为中时,判断新接收的电子邮件发送人是否为白名单用户,如果不是白名单用户,判断新接收的电子邮件中是否包含附件,如果包含附件,将附件发送至沙盒中;如果是白名单用户,不执行操作。

6.根据权利要求5所述的计算机病毒防御系统,其特征在于:所述用户画像模块还用于对用户的计算机操作行为在本地进行加密存储,在确定用户的分类后,删除已存储的计算机操作行为。

7.根据权利要求6所述的计算机病毒防御系统,其特征在于:所述用户画像模块还用于每隔预设时间,重新确定用户的分类。

8.根据权利要求7所述的计算机病毒防御系统,其特征在于:所述用户画像模块还用于记录用户的账号信息,对比同一应用中,用户当前使用的账号信息和已记录的账号信息是否一致,如果不一致,判断为用户切换,在计算机关闭前,将当前防护等级临时设置为高。

一种计算机病毒防御系统

技术领域

[0001] 本发明涉及计算机技术领域，特别涉及一种计算机病毒防御系统。

背景技术

[0002] 随着计算机技术的不断发展，很多病毒工具(例如，后门程序、木马、间谍软件以及广告软件等)利用系统内核中的漏洞将病毒代码植入到系统程序中，从而导致系统瘫痪，给用户操作带来不便，或者导致用户私人信息泄漏，给用户的人身财产安全带来隐患。

[0003] 目前，勒索病毒已经成为当前互联网安全的重点威胁之一，用户计算机一旦被勒索软件渗透，只能通过重装操作系统的方式来解除勒索行为，但用户重要数据文件不能直接恢复；如果用户想要解密这重要文件，需要向黑客支付高额的赎金后方能解密恢复文件，给用户带了极大的危害。而邮件是勒索病毒入侵的重灾区，不法分子通过诱导用户运行邮件附件触发勒索病毒加密用户本地机器上的文件，进而使用解密密码勒索赎金获取收益。

[0004] 针对勒索病毒的主要防御方式为检测和防护：通过对邮件附件进行分析，特征提取，以及通信特征数据的抓取等方式进行检测，并通过恶意程序行为的管控的方式进行防护。通过采取主动防御措施，可以有效降低通过邮件的方式被勒索病毒感染的概率，但是采取主动防御措施，会占用较多的系统资源，拖慢系统的处理速度。

[0005] 因此，目前需要一种减少系统资源占用且拦截效果好的计算机病毒防御系统。

发明内容

[0006] 本发明提供了一种计算机病毒防御系统，能够有效减少系统资源占用。

[0007] 为了解决上述技术问题，本申请提供如下技术方案：

[0008] 一种计算机病毒防御系统，包括：

[0009] 用户画像模块，用于记录用户的计算机操作行为，根据计算机操作行为分析用户的计算机熟悉程度，基于预设的分类规则和计算机熟悉程度确定用户的分类；用户的分类包括低风险用户、中风险用户和高风险用户；

[0010] 等级确定模块，用于根据用户的分类确定当前的防护等级；在防护等级为高时，启用邮件防护模式；在防护等级为低时，关闭邮件防护模块；

[0011] 邮件防护模块，用于在启用邮件防护模式后，判断新接收的电子邮件中是否包含附件，如果包含附件，将附件发送至沙盒中，在沙盒中对附件进行分析，判断附件中是否包含勒索病毒，如果包含勒索病毒，生成报警信息。

[0012] 基础方案原理及有益效果如下：

[0013] 本方案中，通过记录用户的计算机操作行为，再进行分析，可以得出用户对应计算机的熟悉程度，再结合预设的分类规则可以得出用户的分类。例如，用户对计算机的熟悉程度高，从侧面可以看出用户计算机相关的知识较为丰富，对于勒索病毒有一定的了解，可以确定为低风险用户，如果用户对计算机的熟悉程度低，其主动甄别风险的意识相对较差，可以确定为高风险用户。然后，根据用户的分类确定当前的防护等级，例如高风险用户对应防

护等级为高，启用邮件防护模式。在防护等级为高的邮件防护模式下，电子邮件中的附件都会被送入沙盒中，进行分析，从而有效降低通过邮件的方式被勒索病毒感染的概率。在防护等级为低时，关闭邮件防护模块，由用户自行对邮件内容进行判断，可以减少病毒防御系统对系统资源的占用。

[0014] 综上，本方案根据不同的用户采集不同的防护措施，能够减少系统资源占用且拦截效果好。

[0015] 进一步，所述用户画像模块还用于获取计算机存储设备上的文件列表，根据文件列表分析数据重要等级，基于预设的分类规则、计算机熟悉程度和数据重要等级确定用户的分类。

[0016] 当用户在计算机上存储有重要的数据时，例如文档、照片、工程图等，如果感染勒索病毒，危害程度更大，因此，本优选方案中，在确定用户的分类时，增加数据重要等级这一维度，使得用户的分类更能反应真实情况。

[0017] 进一步，所述用户画面模块还用于记录计算机状态信息，基于预设的分类规则、计算机熟悉程度、据重要等级和计算机状态信息确定用户的分类；计算机状态信息包括计算机操作系统信息、软件安装信息和硬件信息。

[0018] 例如计算机操作系统信息反应的操作系统版本较低，存在漏洞可能性大，风险较高，再例如硬件信息反应计算机的配置极高，则可以忽略资源占用的影响。因此，本优选方案中，在确定用户的分类时，增加计算机状态信息这一维度，使得用户的分类更符合用户当前的实际情况。

[0019] 进一步，所述等级确定模块还用于未确定当前的防护等级前，将初始防护等级设置为高；

[0020] 等级确定模块还用于根据用户的分类生成防护等级建议信息；根据获取的用户的防护等级选择信息确定当前的防护等级；其中防护等级建议信息包括建议低防护等级、建议中防护等级或建议高防护等级。

[0021] 由于记录用户的计算机操作行为进行分析需要一定的时间，在分析结果未出来前，将初始防护等级设置为高，能够降低勒索病毒感染的概率。根据用户的分类生成防护等级建议信息，再由用户进行自主选择，为用户提供参考，以用户选择作为最终的防护等级，将最终的决定权交还到用户手中。

[0022] 进一步，所述等级确定模块还用于在防护等级为中时，启用邮件防护模式；

[0023] 邮件防护模块还用于在启用邮件防护模式且防护等级为中时，判断新接收的电子邮件发送人是否为白名单用户，如果不是白名单用户，判断新接收的电子邮件中是否包含附件，如果包含附件，将附件发送至沙盒中；如果是白名单用户，不执行操作。

[0024] 在启用邮件防护模式且防护等级为中时，只对非白名单用户的邮件进行分析，能够平衡系统资源占用以及安全防护。

[0025] 进一步，所述用户画像模块还用于对用户的计算机操作行为在本地进行加密存储，在确定用户的分类后，删除已存储的计算机操作行为。

[0026] 可以避免计算机操作行为被泄露，有效保护用户隐私。

[0027] 进一步，所述用户画像模块还用于每隔预设时间，重新确定用户的分类。

[0028] 通过定期更新，使得用户的分类更能反映当前的情况。

[0029] 进一步,所述用户画像模块还用于记录用户的账号信息,对比同一应用中,用户当前使用的账号信息和已记录的账号信息是否一致,如果不一致,判断为用户切换,在计算机关闭前,将当前防护等级临时设置为高。

[0030] 在默认用户的计算机被其他用户临时使用时,能够区分默认用户与其他临时用户,在临时用户使用时,将当前防护等级临时设置为高,提高防护。

附图说明

[0031] 图1为实施例一种计算机病毒防御系统的示意图。

具体实施方式

[0032] 下面通过具体实施方式进一步详细说明:

[0033] 实施例

[0034] 如图1所示,本实施例的一种计算机病毒防御系统,包括用户画像模块、等级确定模块、邮件防护模块;

[0035] 用户画像模块用于记录用户的计算机操作行为,根据计算机操作行为分析用户的计算机熟悉程度,还用于获取计算机存储设备上的文件列表,根据文件列表分析数据重要等级,还用于记录计算机状态信息,计算机状态信息包括计算机操作系统信息、软件安装信息和硬件信息。用户画面模块还用于基于预设的分类规则、计算机熟悉程度、数据重要等级和计算机状态信息确定用户的分类;用户的分类包括低风险用户、中风险用户和高风险用户;

[0036] 本实施例中,计算机操作行为包括使用杀毒软件、为计算机更新补丁、官方网站下载软件、安装软件过程中去掉安装附带软件选项、安装软件过程中不进行设置等,为不同的计算机操作行为设置不同的分数,例如安装软件过程中去掉安装附带软件选项+2分,安装软件过程中不进行设置-1分,然后根据总得分反应用户的计算机熟悉程度,得分越高用户的计算机熟悉程度越高。文件列表中不同的文件设置不同的得分,总得分越高数据重要等级越高,例如文档、工程图、照片、拍摄的视频为2分,电视剧、电影视频为0.5分。计算机操作系统信息中,不同的操作系统,同样的操作系统不同的版本设置不同的得分,软件安装信息中,不同的软件设置不同的得分,例如恶意软件得负分。分类规则中包括硬件部分和非硬件部分,硬件部分包括设定的阈值,如果硬件信息中计算机的跑分超过设定的阈值,直接分类为高风险用户,此时计算机的性能高,不需要担心资源占用的问题,如果硬件信息中计算机的跑分没有超过设定的阈值,在通过非硬件部分进行分类。非硬件部分为低风险用户、中风险用户和高风险用户划定不同的分数区间,通过上述各项的总得分之和的最终分数,确定所在的分数区间,找到对应的分类。

[0037] 用户画像模块还用于对用户的计算机操作行为在本地进行加密存储,在确定用户的分类后,删除已存储的计算机操作行为。

[0038] 用户画像模块还用于每隔预设时间,重新确定用户的分类。预设时间为6-12个月,本实施例中为6个月。

[0039] 用户画像模块还用于记录用户的账号信息,对比同一应用中,用户当前使用的账号信息和已记录的账号信息是否一致,如果不一致,判断为用户切换,在计算机关闭前,将

当前防护等级临时设置为高。本实施例中，用户的账号信息指用户在计算机上登陆各种软件，网站的账号，当同一网站使用的账号与记录的账号不一致时，判断为用户切换。例如，某网站记录的账号信息为A1111，当前登陆时，使用的账号信息是123456，不一致。在其他实施例中，还可以结合用户的计算机操作行为来判断是否为同一用户注册多个账号的情况。

[0040] 等级确定模块用于根据用户的分类确定当前的防护等级；

[0041] 具体的，根据用户的分类生成防护等级建议信息；其中防护等级建议信息包括建议低防护等级、建议中防护等级或建议高防护等级。本实施例中，低风险用户对应防护等级为低，中风险用户对应防护等级为中，高风险用户对应防护等级为高；例如，当前用户分类为低风险用户，则防护等级建议信息为建议低防护等级；等级确定模块还用于根据获取的用户的防护等级选择信息确定当前的防护等级；例如在建议低防护等级的情况下，用户可以选择低防护等级，也可以选择中或高防护等级。

[0042] 等级确定模块还用于在防护等级为中和高时，启用邮件防护模式；在防护等级为低时，关闭邮件防护模块，以及在未确定当前的防护等级前，将初始防护等级设置为高。

[0043] 邮件防护模块用于在启用邮件防护模式且防护等级为高时，判断新接收的电子邮件中是否包含附件，如果包含附件，将附件发送至沙盒中，在沙盒中对附件进行分析，判断附件中是否包含勒索病毒，如果包含勒索病毒，生成报警信息。

[0044] 邮件防护模块还用于在启用邮件防护模式且防护等级为中时，判断新接收的电子邮件发送人是否为白名单用户，如果不是白名单用户，判断新接收的电子邮件中是否包含附件，如果包含附件，将附件发送至沙盒中；如果是白名单用户，不执行操作。本实施例中，白名单由用户自行添加。

[0045] 以上的仅是本发明的实施例，该发明不限于此实施案例涉及的领域，方案中公知的具体结构及特性等常识在此未作过多描述，所属领域普通技术人员知晓申请日或者优先权日之前发明所属技术领域所有的普通技术知识，能够获知该领域中所有的现有技术，并且具有应用该日期之前常规实验手段的能力，所属领域普通技术人员可以在本申请给出的启示下，结合自身能力完善并实施本方案，一些典型的公知结构或者公知方法不应当成为所属领域普通技术人员实施本申请的障碍。应当指出，对于本领域的技术人员来说，在不脱离本发明结构的前提下，还可以作出若干变形和改进，这些也应该视为本发明的保护范围，这些都不会影响本发明实施的效果和专利的实用性。本申请要求的保护范围应当以其权利要求的内容为准，说明书中的具体实施方式等记载可以用于解释权利要求的内容。

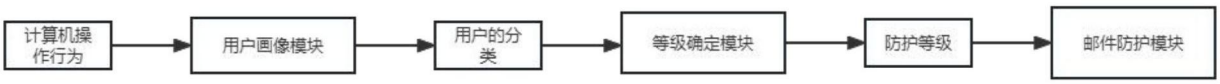

图1