(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 117725630 B
(45)授权公告日 2024.07.09

(21)申请号 202410177273.7
(22)申请日 2024.02.08
(65)同一申请的已公布的文献号
申请公布号 CN 117725630 A
(43)申请公布日 2024.03.19
(73)专利权人 深信服科技股份有限公司
地址 518055 广东省深圳市南山区学苑大道1001号南山智园A1栋
(72)发明人 徐敬蘅 鲍旭华 甘霖 杨航锋 桑瑞强 江达强 姜正文
(74)专利代理机构 北京派特恩知识产权代理有限公司 11270
专利代理师 孙静 徐川
(51)Int.Cl.
G06F 21/78(2013.01)
G06F 21/60(2013.01)
G06F 21/62(2013.01)
(56)对比文件
CN 106484570 A,2017.03.08
US 2018018458 A1,2018.01.18
审查员 赵玉华

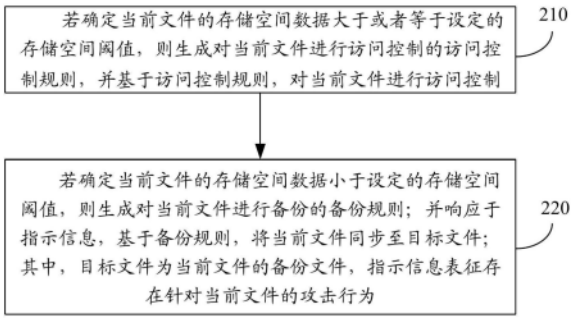
权利要求书2页 说明书36页 附图12页

(54)发明名称

安全防护方法、设备、存储介质和计算机程序产品

(57)摘要

本申请公开了一种安全防护方法、设备、存储介质和计算机程序产品。该方法包括:若确定当前文件的存储空间数据大于或者等于设定的存储空间阈值,则生成对当前文件进行访问控制的访问控制规则,并基于访问控制规则,对当前文件进行访问控制;若确定当前文件的存储空间数据小于设定的存储空间阈值,则生成对当前文件进行备份的备份规则;并响应于指示信息,基于备份规则,将当前文件同步至目标文件;其中,目标文件为当前文件的备份文件,指示信息表征存在针对当前文件的攻击行为。如此,在提升对恶意文件的安全防护能力的同时,降低了安全防护成本。



CN 117725630 B

1.一种安全防护方法,其特征在于,所述方法包括:

若确定当前文件的存储空间数据大于或者等于设定的存储空间阈值,则生成对所述当前文件进行访问控制的访问控制规则,并基于所述访问控制规则,对所述当前文件进行访问控制;

若确定当前文件的存储空间数据小于所述设定的存储空间阈值,则生成对所述当前文件进行备份的备份规则;并响应于指示信息,基于所述备份规则,将所述当前文件同步至目标文件;其中,所述目标文件为所述当前文件的备份文件,所述指示信息表征存在针对所述当前文件的攻击行为;

所述方法还包括:

获取针对当前文件的行为信息;

对所述行为信息进行动态检测,若确定存在针对当前文件的攻击行为,则生成所述指示信息;

其中,所述行为信息包括:加密行为信息;

相应地,所述对所述行为信息进行动态检测,确定存在针对当前文件的攻击行为,包括:

基于针对当前文件的加密行为信息,确定所述当前文件的熵值;

确定所述熵值大于或者等于设定的熵值阈值,则获取除加密行为信息之外的其他行为信息;

基于所述其他行为信息和行为识别模型,生成检测结果,所述检测结果用于表征行为信息是否为攻击行为;所述检测结果包括表征行为信息为攻击行为的第一检测结果,基于所述第一检测结果,生成所述指示信息。

2.根据权利要求1所述的方法,其特征在于,所述方法还包括:

若确定当前时刻为增量同步时刻,则获取所述当前文件的增量同步数据,所述增量同步数据基于所述当前文件的快照信息生成或者基于所述当前文件的增量卷影副本数据生成;

基于所述增量同步数据,更新所述目标文件。

3.根据权利要求2所述的方法,其特征在于,所述方法还包括:

基于当前文件在所述当前时刻对应的数据块信息,生成所述增量卷影副本数据;

基于所述增量卷影副本数据和历史索引关系,生成目标数据块的目标标识信息和增量信息,所述历史索引关系包括:当前文件在上一增量同步时刻对应的数据块的信息;所述目标数据块为所述数据块中的一个或多个;

基于所述目标标识信息和增量信息,生成所述增量同步数据。

4.根据权利要求1所述的方法,其特征在于,所述备份规则包括:卷影阴影复制服务规则,所述基于所述备份规则,将所述当前文件同步至目标文件,包括:

确定所述当前文件的数据在当前时刻发生变化,则暂停当前针对所述当前文件的写操作;

基于所述卷影阴影复制服务规则的卷影阴影复制服务对当前文件及其所在卷的当前时刻的数据进行复制,生成卷影副本数据;

确定所述卷影副本数据生成完成,则恢复所述写操作,并基于所述卷影副本数据,生成

同步数据;

将所述同步数据同步至所述目标文件。

5.根据权利要求1所述的方法,其特征在于,所述访问控制规则包括进程列表和映射关系,所述基于所述访问控制规则,对所述当前文件进行保护,包括:

确定当前进程在所述进程列表中,则允许所述当前进程访问所述当前文件或者获取所述当前进程要访问的当前文件的当前文件目录信息;

确定所述当前进程和所述当前文件目录的对应关系满足所述映射关系,则允许所述当前进程访问所述当前文件目录,所述映射关系包括进程信息与文件目录的对应关系。

6.根据权利要求1所述的方法,其特征在于,所述方法还包括:

响应于所述指示信息,阻断当前进程;

确定将所述当前文件同步至目标文件完成,则基于所述目标文件,生成一键回滚操作指令;

响应于所述一键回滚操作指令,对所述当前文件进行回滚操作,以将所述当前文件恢复至所述目标文件。

7.一种计算机程序产品,包括计算机程序或指令,其特征在于,所述计算机程序或指令被处理器执行时实现权利要求1至6任一项所述方法的步骤。

8.一种电子设备,其特征在于,包括:处理器和用于存储能够在处理器上运行的计算机程序的存储器,其中,

所述处理器,用于运行计算机程序时,执行权利要求1至6任一项所述方法的步骤。

9.一种计算机存储介质,所述计算机存储介质上存储有计算机程序,其特征在于,所述计算机程序被处理器执行时,实现权利要求1至6任一项所述方法的步骤。

安全防护方法、设备、存储介质和计算机程序产品

技术领域

[0001] 本申请涉及网络安全领域,尤其涉及一种安全防护方法、设备、存储介质和计算机程序产品。

背景技术

[0002] 随着通信和互联网技术的快速发展,信息交互更加频繁,各类恶意文件也越来越多。例如,恶意文件包括勒索软件,勒索软件是一种加密或窃取用户数据的病毒恶意攻击方式,它通常以威胁要公布受害者的个人数据或永久阻止访问,要求受害者支付赎金。

[0003] 在相关技术中,用户可以基于静态防护或者动态防护来提高防护能力,但是,仍存在对由于误操作或者安全策略配置不当等导致检测、防护能力被绕过的可能。基于此,可以采用备份方案,通过备份方式将数据及关键系统进行备份,使企业在遭受勒索攻击后无需支付赎金即可快速成功实现数据恢复。

[0004] 但是,随着勒索软件攻击不断演变,传统的备份方案存在一系列的局限性。在相关技术中,传统的备份方案需要投资大量硬件设备以及大量的物理存储介质,在对于需要进行频繁备份和大规模数据恢复的场景下,还需要雇佣专业的备份管理员,其所耗费的成本高,同时在备份的过程中,需要较长的备份窗口时间,备份效率低,从而导致备份不及时,降低了网络安全的防护能力。

发明内容

[0005] 有鉴于此,本申请实施例提供了一种安全防护方法、设备、存储介质和计算机程序产品,旨在提升对恶意文件的安全防护能力的同时,降低安全防护成本。

[0006] 本申请实施例的技术方案是这样实现的:

[0007] 第一方面,本申请实施例提供了一种安全防护方法,所述方法包括:

[0008] 若确定当前文件的存储空间数据大于或者等于设定的存储空间阈值,则生成对所述当前文件进行访问控制的访问控制规则,并基于所述访问控制规则,对所述当前文件进行访问控制;

[0009] 若确定当前文件的存储空间数据小于所述设定的存储空间阈值,则生成对所述当前文件进行备份的备份规则;并响应于指示信息,基于所述备份规则,将所述当前文件同步至目标文件;其中,所述目标文件为所述当前文件的备份文件,所述指示信息表征存在针对所述当前文件的攻击行为。

[0010] 在一些实施例中,所述方法还包括:

[0011] 若确定当前时刻为增量同步时刻,则获取所述当前文件的增量同步数据,所述增量同步数据基于所述当前文件的快照信息生成或者基于所述当前文件的增量卷影副本数据生成;

[0012] 基于所述增量同步数据,更新所述目标文件。

[0013] 在一些实施例中,所述方法还包括:

[0014] 基于当前文件在所述当前时刻对应的数据块信息,生成所述增量卷影副本数据;

[0015] 基于所述增量卷影副本数据和历史索引关系,生成目标数据块的目标标识信息和增量信息,所述历史索引关系包括:当前文件在上一增量同步时刻对应的数据块的信息;所述目标数据块为所述数据块中的一个或多个;

[0016] 基于所述目标标识信息和增量信息,生成所述增量同步数据。

[0017] 在一些实施例中,所述备份规则包括:卷影阴影复制服务规则,所述基于所述备份规则,将所述当前文件同步至目标文件,包括:

[0018] 确定所述当前文件的数据在当前时刻发生变化,则暂停当前针对所述当前文件的写操作;

[0019] 基于所述卷影阴影复制服务规则的卷影阴影复制服务对当前文件及其所在卷的当前时刻的数据进行复制,生成卷影副本数据;

[0020] 确定所述卷影副本数据生成完成,则恢复所述写操作,并基于所述卷影副本数据,生成同步数据;

[0021] 将所述同步数据同步至所述目标文件。

[0022] 在一些实施例中,所述访问控制规则包括进程列表和映射关系,所述基于所述访问控制规则,对所述当前文件进行保护,包括:

[0023] 确定当前进程在所述进程列表中,则允许所述当前进程访问所述当前文件或者获取所述当前进程要访问的当前文件的当前文件目录信息;

[0024] 确定所述当前进程和所述当前文件目录的对应关系满足所述映射关系,则允许所述当前进程访问所述当前文件目录,所述映射关系包括进程信息与文件目录的对应关系。

[0025] 在一些实施例中,所述方法还包括:

[0026] 获取针对当前文件的行为信息;

[0027] 对所述行为信息进行动态检测,若确定存在针对当前文件的攻击行为,则生成所述指示信息;

[0028] 其中,所述行为信息包括:加密行为信息;

[0029] 相应地,所述对所述行为信息进行动态检测,确定存在针对当前文件的攻击行为,包括:

[0030] 基于针对当前文件的加密行为信息,确定所述当前文件的熵值;

[0031] 确定所述熵值大于或者等于设定的熵值阈值,确定存在针对当前文件的攻击行为。

[0032] 在一些实施例中,所述方法还包括:

[0033] 响应于所述指示信息,阻断当前进程;

[0034] 确定将所述当前文件同步至目标文件完成,则基于所述目标文件,生成一键回滚操作指令;

[0035] 响应于所述一键回滚操作指令,对所述当前文件进行回滚操作,以将所述当前文件恢复至所述目标文件。

[0036] 第二方面,本申请实施例还提供了一种计算机程序产品,包括计算机程序或指令,所述计算机程序或指令被处理器执行时实现上述第一方面任一项所述方法的步骤。

[0037] 第三方面,本申请实施例提供了一种电子设备,包括:处理器和用于存储能够在处

理器上运行的计算机程序的存储器,其中,所述处理器用于运行计算机程序时,执行本申请实施例第一方面所述方法的步骤。

[0038] 第四方面,本申请实施例提供了一种计算机存储介质,所述计算机存储介质上存储有计算机程序,所述计算机程序被处理器执行时,实现本申请实施例第一方面所述方法的步骤。

[0039] 本申请实施例提供的技术方案,提供了一种安全防护方法,该方法包括:确定当前文件的存储空间数据是否大于或者等于设定的存储空间阈值,若是,则生成对当前文件进行访问控制的访问控制规则,若否,则生成对当前文件进行备份的备份规则;基于访问控制规则,对当前文件进行访问控制;或者,确定存在针对当前文件的攻击行为,则生成指示信息;响应于指示信息,基于备份规则,将当前文件同步至目标文件。

[0040] 如此,本申请实施例通过主动对大文件进行访问控制规则,以及对小文件,在确定存在攻击行为时,及时对小文件进行备份,实现了备份方案的按需启动。即通过对大文件和小文件采用不同的安全防护方案,提升了对恶意文件的安全防护能力,同时通过备份方案的按需启动,降低了文件的备份成本和安全防护成本,提升了文件的备份效率。

附图说明

[0041] 图1为本申请实施例提供的勒索病毒攻击链的示意图;

[0042] 图2为本申请实施例提供的安全防护方法的流程示意图;

[0043] 图3为本申请实施例提供的访问控制技术的适用对比示意图;

[0044] 图4为本申请实施例提供的增量备份方案的原理示意图;

[0045] 图5为本申请实施例提供的终端客户端基于诱饵文件查杀病毒的流程示意图;

[0046] 图6为本申请实施例提供的勒索行为检测流程图;

[0047] 图7为本申请实施例提供的神经网络提取行为模型的示意图;

[0048] 图8为本申请一应用示例的勒索攻击智能识别与风险响应的系统架构图;

[0049] 图9为本申请一应用示例的采用人机共智理念对抗勒索病毒的流程示意图;

[0050] 图10为本申请一应用示例的GandCrab的代码片段示意图;

[0051] 图11为本申请一应用示例的基于神经网络识别未知病毒的原理示意图;

[0052] 图12为本申请一应用示例的人工智能检测引擎基本原理的示意图;

[0053] 图13为本申请一应用示例的对抗网络学习模型的示意图;

[0054] 图14为本申请一应用示例的多智能体模型推荐架构示意图;

[0055] 图15为本申请一应用示例的勒索攻击备份与数据恢复子系统主体框架;

[0056] 图16为本申请一应用示例的勒索实时动态备份方案;

[0057] 图17为本申请一应用示例的快照卷影备份的基本架构示意图;

[0058] 图18为本申请一应用示例的基于硬件的提供者以实现完整副本拷贝的流程示意图;

[0059] 图19为本申请一应用示例的小文件动态实时备份的流程示意图;

[0060] 图20为本申请一应用示例的基于AI的小文件备份机制的示意图;

[0061] 图21为本申请一应用示例提供的为RDP登录二次认证示意图;

[0062] 图22为本申请实施例提供的安全防护装置的结构示意图;

[0063] 图23为本申请实施例提供的电子设备的结构示意图。

具体实施方式

[0064] 下面结合附图及实施例对本申请再作进一步详细的描述。

[0065] 除非另有定义,本文所使用的所有的技术和科学术语与属于本申请的技术领域的技术人员通常理解的含义相同。本文中在本申请的说明书中所使用的术语只是为了描述具体的实施例的目的,不是旨在于限制本申请。

[0066] 对本申请实施例进行进一步详细说明之前,对本申请实施例中涉及的名词和术语进行说明,本申请实施例中涉及的名词和术语适用于如下的解释:

[0067] 勒索攻击:勒索软件是一种加密或窃取用户数据的病毒恶意攻击方式,它通常以威胁要公布受害者的个人数据或永久阻止访问,要求受害者支付赎金。

[0068] 静态防护:基于计算机二进制文件信息进行扫描的恶意攻击防护方案,通常又称为反病毒;其中计算机二进制文件,包括正常文件(可执行文件,以及office文档、脚本等非可执行文件),以及各类病毒文件(包括但不限于勒索、挖矿、木马、蠕虫等;用户计算机终端感染后,可能带来信息丢失、泄露、计算机终端不可用等后果)。

[0069] 动态防护:基于程序执行行为进行监控,致力于在恶意威胁执行阶段进行阻断的防护方案。程序的执行行为包括但不限于,注册表修改、开启或添加远程控制、进行横向传播、实施文件窃取、加密行为等。

[0070] 未知威胁:广义上讲,指的是未被各大三方平台广泛收录的(静态)病毒文件或(动态)攻击手法;狭义上讲,指的是从未在市面上出现过,未被任何平台、安全厂商甚至(除作者外的)个人收录的病毒文件或攻击手法;本文主要应用其广义含义。

[0071] 卷影复制服务(Volume Shadow Copy Service,VSS):是一项在Microsoft Windows操作系统中提供的关键服务。它旨在解决在备份和恢复过程中出现的数据一致性和可用性的问题。它通过创建卷的“卷影副本”来实现数据备份和恢复功能。卷影副本是指一个卷的快照或镜像,能够提供在数据备份期间保持数据一致性和可访问性的功能。Windows卷影复制服务包括卷影复制提供者(VSS Provider)和卷影副本提供者(VSS Writer)两个核心组件。VSS Provider负责协调和管理卷影副本的创建和恢复,而VSS Writer负责通知VSS Provider在备份和恢复期间需要进行的操作。

[0072] 在相关技术中,以恶意文件为勒索攻击为例,目前勒索病毒得以大规模爆发的原因:一方面是因为勒索的模式套现快、周期短、收入高,而且勒索技术发展快,勒索实施门槛低,有便捷的加密技术供黑客利用,从而吸引着越来越多的技术人才加入勒索病毒背后的黑客团体,黑产由个人化演变为产业化,对于企业的攻击更为频繁与持续,同时比特币、洋葱路由器、动态DNS(Domain Name System,域名系统)等技术的发展使得犯罪分子难以追踪;另一方面,更重要的原因是一些组织安全意识薄弱、安全建设投入不足,黑客容易选择他们作为攻击目标。

[0073] 如今,全球勒索病毒感染态势日益严峻,部分行业及地区已成为勒索软件肆虐的重灾区,给各行各业造成了巨额的经济损失。面对复杂的勒索病毒攻击链,传统的防护方案失效安全形式不容乐观。

[0074] 参照图1,图1为勒索病毒攻击链的示意图,由图1可知,勒索病毒的攻击链一般分

为三大步：

[0075] 第一步：感染病毒。该阶段是指外网到内网的传播，首先进行病毒从外网到内网的感染，该感染包括无文件攻击感染病毒和RDP(Remote Desktop Protocol，远程桌面协议)爆破远程登陆投毒。

[0076] 第二步：加密勒索。漏洞病毒文件运行加密，利用提权，执行提权程度，后执行加密程序，执行加密勒索。

[0077] 第三步：横向传播。最后威胁横向持续扩散，扩大影响面。RDP爆破横向传播，再次加密勒索。

[0078] 目前，面对复杂的勒索病毒攻击，传统的防护方案难以防住。

[0079] 传统备份方案在防御勒索软件方面具有一定的优势和重要性，存在以下几个关键点：

[0080] 1.数据备份：传统备份方案通过定期备份数据，包括文件、数据库和系统配置等，将数据存储在安全的位置。在遭受勒索软件攻击时，可以从备份中恢复受影响的数据，降低数据丢失和业务中断的风险。

[0081] 2.离线备份：传统备份方案通常将备份数据存储在离线介质中，例如磁带或脱机硬盘。这种离线备份方式可以防止勒索软件对备份数据的直接访问和篡改，提供额外的安全层级。

[0082] 3.多版本备份：传统备份方案通常支持多版本备份，即保存多个历史备份的副本。这样可以使组织能够恢复到之前未受到勒索软件攻击的数据状态，减少数据丢失和损坏的影响。

[0083] 4.定期测试和验证备份：传统备份方案需要定期测试和验证备份数据的完整性和可用性。通过进行恢复测试，确保备份数据的可靠性和恢复性，组织可以更有信心地应对勒索软件攻击。

[0084] 5.管理备份访问权限：传统备份方案通常具有访问控制机制，只有授权的用户或管理员可以访问和操作备份数据。通过限制对备份数据的访问权限，可以减少勒索软件对备份数据的风险。

[0085] 备份恢复技术用于对抗勒索病毒很有效，因为由于误操作、安全策略配置不当可能导致检测、防护能力被绕过，所以还需要备份恢复能力做技术兜底。传统数据备份类产品通过备份方式将数据及关键系统进行备份，使企业在遭受勒索攻击后无需支付赎金即可快速成功实现数据恢复。

[0086] 然而，随着勒索软件攻击不断演变，传统备份恢复方案的一系列局限性愈发凸显。在合理性和有效性方面，传统备份恢复方案具有以下局限性：

[0087] 1.备份系统不具备识别勒索加密文件的能力，无论文件是否被加密，备份系统都会进行备份，不仅增加系统的资源占用，而且会导致备份系统中数据受到污染。

[0088] 2.备份系统无法防范勒索攻击，勒索病毒同样会破坏备份数据，导致备份系统的数据库无法使用，给客户造成严重的数据损失。

[0089] 3.备份系统本身大多无法确保备份过程和存储介质的安全性，从而可能导致未授权的访问和数据泄露。

[0090] 在成本控制方面，传统备份恢复方案的局限性如下：

[0091] 1.存储成本:传统备份方案通常要求使用大量的物理存储介质,如磁带或硬盘阵列,来存储备份数据。这些存储介质的购买和维护成本较高,尤其对于需要大容量存储的组织来说,成本会进一步增加。

[0092] 2.硬件成本:为了支持传统备份方案,需要投资大量硬件设备,包括备份服务器、磁带库、磁带驱动器等。这些设备的购买和维护成本都相对较高,对于中小型企业或预算有限的组织而言,可能难以承受。

[0093] 3.人力成本:传统备份方案通常需要专门的人员来管理备份任务、监控备份状态和执行恢复操作。这增加了组织的人力成本,尤其是对于需要进行频繁备份和大规模数据恢复的组织而言,需要雇佣专业的备份管理员。

[0094] 4.时间成本:传统备份方案可能需要较长的备份窗口时间,以完成备份操作。这可能会对业务运行造成干扰,尤其是在高峰期需要持续运行的环境中,备份操作可能与正常业务活动冲突,导致业务中断或降低效率。

[0095] 5.扩展性和灵活性限制:传统备份方案在面对数据增长和变化的需求时可能缺乏灵活性。增加存储容量或适应新的备份需求可能需要额外的硬件投资和配置调整,增加了扩展性和灵活性方面的限制。

[0096] 本申请实施例提供了一种安全防护方法,参照图2,该方法包括如下步骤:

[0097] 步骤210:若确定当前文件的存储空间数据大于或者等于设定的存储空间阈值,则生成对当前文件进行访问控制的访问控制规则,并基于访问控制规则,对当前文件进行访问控制。

[0098] 这里,访问控制(Access Control)指系统对用户身份及其所属的预先定义的策略组限制其使用数据资源能力的手段。通常用于系统管理员控制用户对服务器、目录、文件等网络资源的访问。访问控制是系统保密性、完整性、可用性和合法使用性的重要基础,是网络安全防范和资源保护的关键策略之一,也是主体依据某些访问控制规则对客体本身或其资源进行的不同授权访问。访问控制的主要目的是限制访问主体对客体,例如,用户(主体)对文件(客体)的访问,从而保障数据资源在合法范围内得以有效使用和管理。

[0099] 这里,对于大文件来说,若采用传统的备份方案,会导致备份效率低,存在上述传统备份方案的局限性问题,且安全防护效果不佳。在本申请实施例中,对于大文件,基于访问控制规则,对当前文件进行访问控制。实现了对大文件的主动防护,提升了对恶意文件的安全防护能力。

[0100] 示例性地,以恶意软件为勒索软件为例,参照图3,图3为访问控制技术的适用对比示意图。在图3中,在未限制应用程序与应用数据的访问权限时,勒索病毒不受限制的访问应用数据,对应用数据非法写入与修改,致使正常的应用程序无法识别数据文件内容,数据拥有方无法访问该应用数据。而在防勒索系统中通过建立系统中可信应用与数据的访问关系模型,阻断勒索病毒对应用数据的读写删改、保护系统中文档、数据库、工程文件、音频、图像、视频、配置文件免遭勒索软件恶意加密,数据拥有方可以正常访问应用数据。

[0101] 本申请实施例基于访问控制的大文件保护,实现对恶意文件的防护的方案,具有以下意义:

[0102] (1)防止未经授权的访问:勒索软件通常通过获取未经授权的访问权限来加密或损坏文件。基于访问控制的大文件保护技术可以限制对大型文件的访问权限,确保只有授

权的用户能够访问和操作这些文件。这样可以阻止勒索软件获取到目标文件并对其进行恶意操作。

[0103] (2)限制权限和特权的滥用:勒索软件往往利用特权用户或管理员的权限来加密或删除文件。基于访问控制的大文件保护技术可以确保仅有合适的用户或角色能够获得高权限访问权限,限制了恶意行为者在系统中的操作能力。

[0104] (3)快速发现和应对:基于访问控制的大文件保护技术通常包括审计和监控机制,可以记录和监测对大型文件的访问活动。这样,当勒索软件尝试访问或修改受保护的文件时,可以及时发现异常行为,并采取快速的反应措施,例如中断非授权访问或及时报警。

[0105] (4)敏感数据保护:大型文件通常包含组织的敏感数据。基于访问控制的大文件保护技术可以确保只有授权的用户或角色能够访问和操作这些文件,保护敏感数据免受勒索软件的威胁。

[0106] 因此,本系统所设计的基于访问控制的大文件保护对防御勒索软件具有重要的意义。通过限制未经授权的访问、限制权限滥用、及时发现异常行为、实施数据备份和保护敏感数据,可以有效减少勒索软件对大型文件的威胁,并保护组织的数据和业务免受勒索软件攻击的影响。

[0107] 这里,当前文件的存储空间数据大于或者等于设定的存储空间阈值时,则表明当前文件的存储空间较大,为大文件。对于每一文件来说,都会预先设定其对应的访问控制规则。

[0108] 步骤220:若确定当前文件的存储空间数据小于设定的存储空间阈值,则生成对当前文件进行备份的备份规则;并响应于指示信息,基于备份规则,将当前文件同步至目标文件;其中,目标文件为当前文件的备份文件,指示信息表征存在针对当前文件的攻击行为。

[0109] 这里,由于误操作、安全策略配置不当可能导致检测、防护能力被绕过等问题,因此,在对大文件进行基于访问控制的保护之外,针对其他大量的小文件,还需要备份方案做技术兜底。

[0110] 这里,若当前文件的存储空间数据大于或者等于设定的存储空间阈值时,即当前文件为小文件时,本申请实施例会针对当前文件的攻击行为进行安全检测,任何针对小文件的操作,均会触发防勒索的安全检查,对可信应用文件操作放行,非可信应用文件操作将触发备份动作,生成指示信息,指示信息表征存在针对当前文件的攻击行为。

[0111] 这里,目标文件为当前文件的备份文件,在当前文件的存储空间数据小于设定的存储空间阈值,表明当前文件为小文件,生成对当前文件进行备份的备份规则;并响应于指示信息,基于备份规则,将当前文件同步至目标文件。

[0112] 这里,小文件的备份方案,不是全盘备份,而是配合攻击行为检测的实时动态备份,实现小文件备份的按需触发,既可以实现对攻击行为的精准防范,又能备份缓解攻击行为拦截时损失的少量文件,还能确保最小的系统资源消耗。这里,数据备份是确保数据完整性和可用性的关键因素,尤其是在数据丢失或系统故障的情况下。

[0113] 如此,本申请实施例通过主动对大文件进行访问控制规则,以及对小文件,在确定存在攻击行为时,及时对小文件进行备份,实现了备份方案的按需启动。即通过对大文件和小文件采用不同的安全防护方案,提升了对恶意文件的安全防护能力,同时通过备份方案的按需启动,降低了文件的备份成本和安全防护成本,提升了文件的备份效率。

[0114] 在一些实施例中,该方法还包括:

[0115] 若确定当前时刻为增量同步时刻,则获取当前文件的增量同步数据,增量同步数据基于当前文件的快照信息生成或者基于当前文件的增量卷影副本数据生成;

[0116] 基于增量同步数据,更新目标文件。

[0117] 这里,本申请实施例还可以针对大文件和小文件,定时进行增量备份,实现对文件的多重备份管理,进一步提升对恶意文件的安全防护能力。示例性地,在大文件的访问控制被绕过或者小文件的实时备份失败的情况下,定期增量备份可以进一步提升对恶意文件的安全防护能力。

[0118] 这里,增量同步时刻可以预先设定,在确定当前时刻为增量同步时刻时,开始进行增量同步。

[0119] 这里,获取当前文件的增量同步数据,增量同步数据基于当前文件的快照信息生成或者基于当前文件的增量卷影副本数据生成。这里的增量同步数据是指当前文件在当前时刻相较于上一增量同步时刻的数据的变化数据,这里的变化数据是指增加、删除和修改数据。基于增量同步数据,更新目标文件,以进行当前文件的增量同步备份。

[0120] 这里,增量同步数据基于当前文件的快照信息生成或者基于当前文件的增量卷影副本数据生成。快照信息通常是指文件系统或存储系统在某一特定时间点的状态记录。它会记录下当时所有文件和目录的元数据及内容,形成一个静态视图。在增量同步场景中,基于快照信息生成的增量同步数据是指从上一次快照到当前快照之间文件系统内容变化的部分。增量卷影副本数据则是指在一个或多个时间点上,文件或数据块相对于其原始版本的更改记录。它侧重于记录数据变化的过程,即只保存自上次同步以来发生变化的数据块,而非整个文件系统的全量状态。

[0121] 示例性地,请参照图4,图4为增量备份方案的原理示意图。在图4中,增量备份方案包括:快照增量备份去重技术和基于卷设备的索引机制。快照增量备份去重技术实时记录客户端本地被修改的数据块位置,仅备份被记录的数据块,未被适用的数据块不会被索引和备份。基于快照的增量备份去重方案是终端主机数据备份与恢复系统中的一项关键技术。快照技术的作用主要包括:1)能够进行在线数据恢复,当存储设备发生应用故障或者文件损坏时可以进行及时数据恢复,将数据恢复成快照产生时间点的状态;2)快照的另一个作用是为存储用户提供了另外一个数据访问通道,当原数据进行在线应用处理时,用户可以访问快照数据,还可以利用快照进行测试等工作。

[0122] 创建快照的主要步骤包括:1)首先发起创建指令;2)在发起时间点,指令通知操作系统暂停应用程序和文件系统的操作;3)刷新文件系统缓存,结束所有的读写事务;4)创建快照点;5)创建完成之后,释放文件系统和应用程序,系统恢复正常运行。

[0123] 例如,对于一些大型数据库文件,在使用过程中通常只会更改其中的部分数据。基于快照的增量备份方案能够准确识别被修改的数据块位置,只备份对应的修改块,而无需将整个数据库文件进行备份。这种精确备份的方式极大地减少了备份数据的量,进而提高了备份效率,并显著降低了备份所需的存储空间。

[0124] 另一方面,终端主机数据备份与恢复系统还采用基于卷设备的索引机制。卷设备索引机制是一种在数据备份和恢复过程中使用的关键技术,旨在提高数据恢复的效率和准确性。它的目标是记录备份数据的位置和相关信息,以便在恢复过程中能够快速定位到所

需的数据块。通过建立索引,恢复操作可以直接访问索引并定位到需要恢复的数据,相较于快照增量备份技术,而无需遍历整个备份数据集,从而提高数据恢复的效率和准确性。

[0125] 如图4所示,卷设备的索引机制在时刻2023/6/9 12:12:11:1创建快照(首次全量快照)时会对磁盘簇创建一个卷设备索引表,在时刻2023/6/9 12:12:11:2对新增变化数据进行增量同步时,该卷设备索引表可以高效定位到特定的数据块(例如1010)及其历史版本,尤其对于实现细粒度恢复(如按文件、按时间点恢复),并对其进行复写,并备份被复写数据,复写没有覆盖原先的簇,是不会产生额外的备份空间,从而大大节省了备份空间占用。

[0126] 如此,通过对当前文件进行定时增量备份,以应对大文件存在的由于误操作或者访问控制规则不当等导致检测、防护能力被绕过时产生的攻击行为,同时对小文件来说,实现对文小件的多重备份管理,进一步提升了对恶意文件的安全防护能力。

[0127] 在一些实施例中,该方法还包括:

[0128] 基于当前文件在当前时刻对应的数据块信息,生成增量卷影副本数据;

[0129] 基于增量卷影副本数据和历史索引关系,生成目标数据块的目标标识信息和增量信息,历史索引关系包括:当前文件在上一增量同步时刻对应的数据块的信息;目标数据块为数据块中的一个或多个;

[0130] 基于目标标识信息和增量信息,生成增量同步数据。

[0131] 这里,在基于VSS备份技术进行数据备份和同步场景中,首先,系统会检测当前文件的所有数据块,并记录每个数据块在当前时间点的状态(内容、修改时间等)。对比上次创建卷影副本的时间点,系统只选择那些发生变化的数据块进行捕获,形成新的增量数据。这些变化的数据块被整合在一起,生成一个增量卷影副本,该副本仅包含自上一同步后更改的内容。

[0132] 这里,历史索引关系是指存储了在上一次增量同步时每个数据块状态的元数据信息。系统通过比较新产生的增量卷影副本与历史索引中的数据块信息,识别出哪些数据块是新增、删除或修改过的。对于每一个有变动的数据块即目标数据块,目标数据块为数据块中的一个或多个,生成相应的目标标识信息,目标标识信息包括数据块的位置、大小以及在目标存储位置的新标识符等。增量信息则包含了这些数据块从上一次同步到现在实际内容的差异,以便在目标端应用这些变更。

[0133] 这里,根据目标标识信息,可以知道在目标存储位置应该更新哪些数据块。同步过程中,系统利用增量信息将源端数据块的改动精确地应用到目标端相应的位置。

[0134] 如此,相较于传统文件级的备份方式在海量小文件或文件有大量碎片的情况下,读文件时将耗费大量磁盘寻道时间,导致备份速度非常低。基于卷影复制技术备份时会绕过文件系统,直接在卷设备上按需拷贝数据,而且产生的增量写入如果没有覆盖原先的磁盘簇,是不会产生额外的备份空间,从而大大提高了备份性能,并且节省了备份空间的占用。

[0135] 在一些实施例中,备份规则包括:卷影阴影复制服务规则,基于备份规则,将当前文件同步至目标文件,包括:

[0136] 确定当前文件的数据在当前时刻发生变化,则暂停当前针对当前文件的写操作;

[0137] 基于卷影阴影复制服务规则的卷影阴影复制服务对当前文件及其所在卷的当前

时刻的数据进行复制,生成卷影副本数据;

[0138] 确定卷影副本数据生成完成,则恢复写操作,并基于卷影副本数据,生成同步数据;

[0139] 将同步数据同步至目标文件。

[0140] 这里,本申请实施例若确定存在攻击行为,对小文件采用实时动态备份方案,将当前文件同步至目标文件。确定当前文件的数据在当前时刻发生变化,则触发备份动作,并且为了保证数据的一致性,暂停当前针对当前文件的写操作。

[0141] 这里,备份规则包括:卷影阴影复制服务规则,卷影阴影复制服务(VSS)被触发,它与文件系统和其他相关组件协调,创建一个该文件及其所在卷在当前时刻的一致性快照。这里的“卷”指的是计算机存储设备(如硬盘、固态硬盘等)上的一个逻辑分区或存储区域。在Windows操作系统或其他支持磁盘分区的操作系统中,一个物理硬盘可以被划分为一个或多个逻辑卷,每个卷都有自己的驱动器号(例如C:\、D:\等),并使用独立的文件系统进行格式化和管理。传统的文件级备份方式需要读取和写入大量小文件,这会导致磁盘寻道时间增加,因为磁头需要频繁移动来读取不同的物理位置。卷影复制技术直接在卷设备上进行操作,绕过了文件系统这一层级,减少了磁头的移动,从而提高了备份速度。

[0142] 这里,要对文件进行备份操作,那么卷影阴影复制服务会处理整个卷以确保数据的一致性,这意味着它不仅复制单个文件,还复制了与该文件相关的卷上所有相关元数据和其他信息,以保证在创建备份时数据是完整的且处于一致状态。

[0143] 这里,使用生成的卷影副本数据,对比上一次备份或同步时的目标文件状态,提取出自上次同步以来所有新增、修改或删除的数据块信息。根据这些差异,生成包含增量更改的同步数据包。

[0144] 这里,将上述同步数据包传输到目标存储位置,并在那里应用这些更改,从而更新目标文件的内容,使其与源文件最新的卷影副本保持一致。在目标文件所处的目标端,根据同步数据中的指示更新目标文件对应的各个数据块,最终实现增量同步。通过这种方式,VSS不仅能够在不影响正常业务运行的情况下进行数据备份,而且还可以高效地执行增量数据同步任务。

[0145] 如此,通过卷影阴影复制服务规则,在确定存在攻击行为时,对小文件进行实时动态备份,将同步数据实时同步至目标文件,在实现攻击行为精准防范的同时,又能备份缓解行为拦截时损失的文件以及确保在攻击行为成功后,能够及时恢复数据,还能确保最小的系统资源消耗,提升了对恶意文件的安全防护能力。

[0146] 在一些实施例中,访问控制规则包括进程列表和映射关系,基于访问控制规则,对当前文件进行保护,包括:

[0147] 确定当前进程在进程列表中,则允许当前进程访问当前文件或者获取当前进程要访问的当前文件的当前文件目录信息;

[0148] 确定当前进程和当前文件目录的对应关系满足映射关系,则允许当前进程访问当前文件目录,映射关系包括进程信息与文件目录的对应关系。

[0149] 这里,当前进程尝试访问某个文件时,操作系统会首先检查该进程的有效用户ID和有效组ID是否在进程列表中,则表明该进程具有对该文件的适当权限(如读、写、执行等)。

[0150] 或者对进程访问的目录进行限制,获取当前进程要访问的当前文件的当前文件目录信息,进程只被允许访问特定的文件目录集合。

[0151] 示例性地,针对需要安全性极高的目录/文件,设计可信进程防护机制,除了允许的进程可以运行之外,其他所有的进程都不能运行,适用于对安全性要求极高的场景。开启可信进程防护之后,在可信进程列表的进程可以运行,不在可信进程列表的进程则不能运行,可信进程防护有两种模式:

[0152] 服务器系统:在可信进程列表中的进程,可以访问服务器系统的所有文件。

[0153] 服务器特定目录:在可信进程列表中的进程可以访问指定目录下的文件,非指定目录下的文件不能访问。

[0154] 在开启“服务器系统/服务器特定目录”可信进程防护后,将在后台自动学习一段时间服务器中的进程列表,并将这些进程列表作为白基线,可以访问服务器中的所有文件/服务器特定目录。其他进程作为非法进行不能访问服务器中的文件/服务器特定目录。如此,通过可信进程防护机制,对大文件进行访问控制,可以减少勒索软件对大文件的风险,提升了大文件对恶意文件的安全防护能力。

[0155] 此外,虽然VSS是一种功能强大的Windows服务,但勒索软件同样可能利用其漏洞和弱点来破坏数据备份完整性。删除VSS是一种常见的攻击方式,攻击者可以利用特权访问或恶意软件来删除已创建的VSS快照,从而破坏数据的恢复能力。常见的删除VSS的攻击方式包括:攻击者通过获取管理员权限或其他高权限用户的凭证,可以访问和操作VSS服务,包括删除已创建的快照。恶意软件可能以管理员权限运行,通过调用相关的API或命令来删除VSS快照。这可以导致数据备份不完整,使恢复变得困难或不可能。

[0156] 在一些实施例中,也可以对备份区以及卷影实现高级别自保护,例如,带有签名的才让访问被分去以及卷影,确保备份文件与卷影万无一失。

[0157] 在一些实施例中,访问控制规则包括一个或多个,基于访问控制规则,对当前文件进行保护,包括:

[0158] 获取针对当前文件的文件访问信息,文件访问信息包括:访问用户信息、访问类型和访问等级;

[0159] 基于文件访问信息,确定一个或多个访问控制规则中的目标访问控制规则,其中,一个或多个访问控制规则至少包括:自主访问控制规则、强制访问控制规则和基于角色访问控制规则;

[0160] 基于目标访问控制规则,对当前文件进行访问控制。

[0161] 这里,文件访问信息包括:访问用户信息、访问类型和访问等级;访问用户信息:通常指的是进程的有效用户ID和有效组ID,代表了请求访问文件的进程的身份。访问类型:包括读(read)、写(write)、执行(execute)以及可能的附加权限,如删除、重命名等。访问等级:在某些系统中,可以进一步细分为不同的访问级别。

[0162] 需要说明的是,访问控制规则包括三个要素:主体、客体和控制策略。

[0163] (1)主体S(Subject)。是指提出访问资源具体请求。是某一操作动作的发起者,但不一定是动作的执行者,可能是某一用户,也可以是用户启动的进程、服务和设备等。

[0164] (2)客体O(Object)。是指被访问资源的实体。所有可以被操作的信息、资源、对象都可以是客体。客体可以是信息、文件、记录等集合体,也可以是网络上硬件设施、无限通信

中的终端,甚至可以包含另外一个客体。

[0165] (3)控制策略A(Access Control Policy)。是主体对客体的相关访问规则集合,即属性集合。访问策略体现了一种授权行为,也是客体对主体某些操作行为的默认。

[0166] 访问控制的主要功能包括:保证合法用户访问受权保护的网络资源,防止非法的主体进入受保护的网络资源,或防止合法用户对受保护的网络资源进行非授权的访问。访问控制首先需要对用户身份的合法性进行验证,同时利用控制策略进行选用和管理工作。当用户身份和访问权限验证之后,还需要对越权操作进行监控。因此,访问控制的内容包括认证、控制策略实现和安全审计。

[0167] (1)认证。包括主体对客体的识别及客体对主体的检验确认。

[0168] (2)控制策略。通过合理地设定控制规则集合,确保用户对信息资源在授权范围内的合法使用。既要确保授权用户的合理使用,又要防止非法用户侵权进入系统,使重要信息资源泄露。同时对合法用户,也不能越权行使权限以外的功能及访问范围。

[0169] (3)安全审计。系统可以自动根据用户的访问权限,对计算机网络环境下的有关活动或行为进行系统的、独立的检查验证,并做出相应评价与审计。

[0170] 主要的访问控制类型有3种模式:自主访问控制(Discretionary Access Control,DAC)、强制访问控制(Mandatory Access Control,MAC)和基于角色访问控制(Role-Based Access Control,RBAC)。

[0171] 1)自主访问控制

[0172] 自主访问控制(DAC)是一种接入控制服务,通过执行基于系统实体身份及其到系统资源的接入授权。包括在文件,文件夹和共享资源中设置许可。用户有权对自身所创建的文件、数据表等访问对象进行访问,并可将其访问权授予其他用户或收回其访问权限。允许访问对象的属主制定针对该对象访问的控制策略,通常可通过访问控制列表来限定针对客体可执行的操作。

[0173] ①每个客体有一个所有者,可按照各自意愿将客体访问控制权限授予其他主体。

[0174] ②各客体都拥有一个限定主体对其访问权限的访问控制列表(ACL)。

[0175] ③每次访问时都以基于访问控制列表检查用户标志,实现对其访问权限控制。

[0176] ④DAC的有效性依赖于资源的所有者对安全政策的正确理解和有效落实。

[0177] DAC提供了适合多种系统环境的灵活方便的数据访问方式,是应用最广泛的访问控制策略。然而,它所提供的安全性可被非法用户绕过,授权用户在获得访问某资源的权限后,可能传送给其他用户。主要是在自由访问策略中,用户获得文件访问后,若不限制对该文件信息的操作,即没有限制数据信息的分发。所以DAC提供的安全性相对较低,无法对系统资源提供严格保护。

[0178] 2)强制访问控制

[0179] 强制访问控制(MAC)是系统强制主体服从访问控制策略。是由系统对用户所创建的对象,按照规定的规则控制用户权限及操作对象的访问。主要特征是对所有主体及其所控制的进程、文件、段、设备等客体实施强制访问控制。在MAC中,每个用户及文件都被赋予一定的安全级别,只有系统管理员才可确定用户和组的访问权限,用户不能改变自身或任何客体的安全级别。系统通过比较用户和访问文件的安全级别,决定用户是否可以访问该文件。此外,MAC不允许通过进程生成共享文件,以通过共享文件将信息在进程中传递。MAC

可通过使用敏感标签对所有用户和资源强制执行安全策略,一般采用3种方法:限制访问控制、过程控制和系统限制。MAC常用于多级安全军事系统,对专用或简单系统较有效,但对通用或大型系统并不太有效。

[0180] MAC的安全级别有多种定义方式,常用的分为4级:绝密级(Top Secret)、秘密级(Secret)、机密级(Confidential)和无级别级(Unclas sified),其中T>S>C>U。所有系统中的主体(用户,进程)和客体(文件,数据)都分配安全标签,以标识安全等级。

[0181] 通常MAC与DAC结合使用,并实施一些附加的、更强的访问限制。一个主体只有通过自主与强制性访问限制检查后,才能访问其客体。用户可利用DAC来防范其他用户对自己客体的攻击,由于用户不能直接改变强制访问控制属性,所以强制访问控制提供了一个不可逾越的、更强的安全保护层,以防范偶然或故意地滥用DAC。

[0182] 3)基于角色的访问控制

[0183] 角色(Role)是一定数量的权限的集合。指完成一项任务必须访问的资源及相应操作权限的集合。角色作为一个用户与权限的代理层,表示为权限和用户的关系,所有的授权应该给予角色而不是直接给用户或用户组。

[0184] 基于角色的访问控制(Role-Based Access Control,RBAC)是通过对角色的访问所进行的控制。使权限与角色相关联,用户通过成为适当角色的成员而得到其角色的权限。可极大地简化权限管理。为了完成某项工作创建角色,用户可依其责任和资格分派相应的角色,角色可依新需求和系统合并赋予新权限,而权限也可根据需要从某角色中收回。减小了授权管理的复杂性,降低管理开销,提高企业安全策略的灵活性。

[0185] RBAC模型的授权管理方法,主要有3种:

[0186] ①根据任务需要定义具体不同的角色。

[0187] ②为不同角色分配资源和操作权限。

[0188] ③给一个用户组(Group,权限分配的单位与载体)指定一个角色。

[0189] RBAC支持三个著名的安全原则:最小权限原则、责任分离原则和数据抽象原则。前者可将其角色配置成完成任务所需要的最小权限集。第二个原则可通过调用相互独立互斥的角色共同完成特殊任务,如核对账目等。后者可通过权限的抽象控制一些操作,如财务操作可用借款、存款等抽象权限,而不用操作系统提供的典型的读、写和执行权限。这些原则需要通过RBAC各部件的具体配置才可实现。

[0190] 访问控制机制是检测和防止系统未授权访问,并对保护资源所采取的各种措施。是在文件系统中广泛应用的安全防护方法,一般在操作系统的控制下,按照事先确定的规则决定是否允许主体访问客体,贯穿于系统全过程。

[0191] 这里,基于文件访问请求和预先设定的各种访问控制规则,最终确定出适用于当前情况的目标访问控制规则,确定一个或多个访问控制规则中的目标访问控制规则,其中,一个或多个访问控制规则至少包括:自主访问控制规则、强制访问控制规则和基于角色访问控制规则;基于目标访问控制规则,对当前文件进行访问控制。

[0192] 如此,通过采用多种访问控制规则,对文件进行访问控制,确保了文件的安全性和数据保护,当前进一步提升了大文件的安全防护能力。

[0193] 在一些实施例中,为了进一步提升文件的安全防护能力,包括大文件和小文件,可以采用轻量级分组密码算法对文件进行加密保护。

[0194] 现有的文件加密方式主要可分为三类:第一类是密文覆盖原文,勒索软件读取文件内容并加密,直接写回原文件中;第二类是新建密文后删除原文,勒索软件将加密后的密文写入新文件,并将原文件删除;第三类和第二类的区别在于最后是以覆盖原文件的方式删除原文件。

[0195] 本申请实施例主要使用三种主流的轻量级分组密码算法设计防御手段,分别是CLEFIA(ComplementaryLightweightEnhancedForwardIntegrityArchitecture,克利菲亚)、PRESENT(PRFEctSecureEfficientNtworksTiny,普雷斯恩特)和LEA(LightweightEncryptionAlgorith,轻量级加密)三种分组密码算法。针对数据窃取攻击,主要分为两大类。一类是数据修改的方法,通过在原始数据中添加扰动或采用加密技术来保护训练数据。另一类是模型修改方法,通过修改模型参数来防止数据泄露,该类方法是数据沙箱模式下一种可行的防御方法。我们将两者相结合来增强对数据窃取的抵抗能力。

[0196] 轻量级分组密码算法与传统分组密码算法相比,具有分组长度更小、密钥长度更小、轮函数更简单和密钥编排更简单等几大优点。其中CLEFIA加密算法CLEF由数据处理部分和密钥扩展部分组成,它的基本结构是一种广义Feistel结构,是传统Feistel结构的变形,由四条输入分支组成,每一轮中有两个F函数,每个F函数使用两个不同的S盒和两个不同的扩散矩阵。密钥扩展部分与数据处理部分共享Feistel(费斯脱尔)结构,这使得CLEFIA只需要较小的硬件和软件规模。该算法很显著的特点是代码紧凑,执行速度快,同时也没有损害安全性。与广泛使用的传统分组密码相比,CLEFIA在硬件实现上更有优势。且CLEFIA的设计在安全性、速度、实现成本三个基本方面达到了很好的平衡。而PRESENT分组密码算法采用SPN结构,分组长度为64位,支持80位、128位两种密钥长度。共迭代31轮,每轮的轮函数F由轮密钥加、S盒代换、P置换3部分组成。该算法具有出色的硬件实现性能和简洁的轮函数设计。LEA分组密码算法分为密钥扩展、轮函数的应用和迭代、以及最终的密文生成过程。与传统的分组密码算法相比具有更小的实现规模、更快的加密速度、较高的安全性和较简单的算法结构。

[0197] 针对这些轻量级分组密码算法的数据防窃取的具体防御手段如下:

[0198] 1)数据修改方法:向原始数据中添加随机噪声或用新样本扩展数据集的方法,该方法隐藏单个样本的属性或一组样本的统计特性的敏感信息。使用同态加密技术实现隐私数据的加密计算,使数据分析人员在不接触原始数据的前提下实现模型训练或数据分析。采用区块链实现数据搜索过程中的隐私保护。进一步,直接在密文上训练深度学习模型的完全同态加密方案。利用Paillier加密系统(帕里耶加密系统)将SVM(Support Vector Machine,支持向量机)决策函数转换为密文计算,该方案中测试数据也被加密,所有计算都在密文上进行。可以分别在数据发布和数据传输过程中加密数据,设计了能够防御数据窃取攻击的系统架构。

[0199] 2)模型修改方法:通过修改模型的梯度、参数或输出结果来保护训练数据隐私信息。提出一种随机梯度下降算法,利用差分隐私对模型参数的梯度进行加噪,保证了模型参数不会暴露太多隐私。通过添加噪声来修改模型参数,以去除关于特定训练数据集的信息。在模型的输出中以一定的概率加入噪声,用于预防成员推断攻击,其效果能够使成员推断攻击的成功率降低到50%。另外,为了防止训练数据的模型记忆过多数据,对模型训练算法本身进行修改。提出一种将模型学习算法转化为求和的形式来遗忘训练数据的方法;一种

基于模型叠加的防御方法,用于防御对机器学习模型的攻击,以避免单个模型对训练数据的过度记忆。针对边缘计算和联邦学习的新场景,在参数聚合的过程中增加噪声实现隐私保护。

[0200] 此外,针对CLEFIA、PRESENT和LEA这三个轻量级分组密码算法,数据窃取攻击的防御手段还包括以下几点:

[0201] 密钥管理:密钥的保护和管理对于保障数据安全非常关键。要确保密钥的生成、存储、传输和更新等环节都有严格的安全措施,防止密钥泄露或被恶意攻击者篡改。

[0202] 侧信道防护:轻量级分组密码算法在实现时要防范侧信道攻击,如功耗分析、电磁分析等。通过硬件和软件的相互配合,例如平衡电路设计、随机延迟等措施,可以降低侧信道攻击的风险。

[0203] 抗篡改硬件设计:在实现轻量级分组密码算法的硬件中,采用抗篡改设计,例如使用安全芯片、物理非可克隆函数(PUF)等技术,以防止攻击者通过物理手段破解设备。

[0204] 安全协议与认证:通过使用安全的通信协议以及强身份认证机制,确保数据在传输过程中不被窃取或篡改。

[0205] 在一些实施例中,该方法还包括:

[0206] 获取针对当前文件的行为信息;

[0207] 对行为信息进行动态检测,若确定存在针对当前文件的攻击行为,则生成指示信息;

[0208] 其中,行为信息包括:加密行为信息;

[0209] 相应地,对行为信息进行动态检测,确定存在针对当前文件的攻击行为,包括:

[0210] 基于针对当前文件的加密行为信息,确定当前文件的熵值;

[0211] 确定熵值大于或者等于设定的熵值阈值,确定存在针对当前文件的攻击行为。

[0212] 这里,可以采用数据采集模块监控和响应针对当前文件的行为信息。该行为信息主要包含采集信息爆破攻击事件、文件落地、注册表项、命令执行、进程API、文件追踪、资源占用、网络行为、加密行为等。其主要来自终端上采集的二进制内容(文件、网络流量、内存快照等)、日志(WindowsEventLog、防火墙日志、Web日志等)、事件和监控记录(进程行为、账户活动等),它们被采集、存储、分析和处理,用于作为原始输入,实现终端安全的各类检测和防护方案。数据采集模块主要采用两种技术方案进行获取:

[0213] 1、内核态实时监控:数据采集模块通过内核消息订阅、MiniFilter(微过滤器)、WFP(Windows Filtering Platform,Windows过滤平台)等来实现进程行为的实时监控。优点:监控点单一(无需在用户态影响应用程序);单个事件覆盖率最高;可在内核态过滤,提高事件处理性能;可同步监控,进行拦截防护;可对用户态的对抗免疫。

[0214] 2、用户态HOOK(非内核态):通过将监控代码注入到应用程序中,以API调用为监控点。优点:一些事件只能通过该技术采集;上层事件信息比较完整详细;可做效果和性能之间的灵活平衡;可同步监控进行拦截防护。HOOK通常是指一种用于拦截并修改或增强系统调用、函数调用或消息传递的技术。

[0215] 这里,本申请实施例采用的动态防护方案确定是否存在针对当前文件的攻击行为,若确定存在针对当前文件的攻击行为,则生成指示信息。

[0216] 如此,通过进行动态检测,确定是否存在针对当前文件的攻击行为,实现了对恶意

文件的攻击行为进行动态防护,及时将攻击行为阻断恶意威胁执行阶段。

[0217] 在一些实施例中,其中,行为信息包括:加密行为信息;相应地,对行为信息进行动态检测,确定存在针对当前文件的攻击行为,包括:

[0218] 基于针对当前文件的加密行为信息,确定当前文件的熵值;

[0219] 确定熵值大于或者等于设定的熵值阈值,确定存在针对当前文件的攻击行为。

[0220] 这里,为了实现隐藏自身、加密受害者主机文件以及索取赎金等核心目的,勒索软件通常会对文件进行频繁的操作,并呈现出显著的异常特征。文件被加密时,文件熵(描述混乱程度)会显著增加。

[0221] 这里,利用该特征,本申请实施例确定熵值大于或者等于设定的熵值阈值,即在文件熵显著增加时,确定存在针对当前文件的攻击行为,自动启动内存备份功能。

[0222] 如此,通过基于信息熵的攻击识别与备份触发技术,对攻击行为进行动态监测,确定存在针对当前文件的攻击,提升了对攻击行为的检测能力。

[0223] 在一些实施例中,当前文件包括诱饵文件,对行为信息进行动态检测,确定存在针对当前文件的攻击行为,包括:

[0224] 确定存在针对诱饵文件的行为,则确定存在针对当前文件的攻击行为。

[0225] 这里,参照图5,图5为终端客户端基于诱饵文件查杀病毒的流程示意图。勒索病毒在入侵主机会进行横向传播扩散,影响范围十分广泛,一台终端中毒,全网业务瘫痪。为监控异常文件操作,通过在系统关键目录,放置诱饵文件,并且保证这些诱饵文件会被优先枚举到,当有勒索程序对诱饵文件进行修改或删除时,将触发驱动拦截该进程行为,并将该进程信息上报给应用层进行病毒文件查杀。

[0226] 在图5中,本申请实施例通过对上万种勒索软件加密顺序进行研判后筛选出攻击行为大概率优先加密的关键目录,在实际应用中,1.终端客户端在系统关键目录及随机目录放置诱饵文件;2.诱饵文件将加密进程反馈至客户端;3.杀掉加密进程阻止加密。4.查杀病毒源文件。

[0227] 本申请实施例通过基于诱饵文件的针对性的勒索诱捕方案,主动进行勒索病毒的防御,及时阻止了病毒的大范围传播,全面阻止业务不可逆终端,保护主机安全。

[0228] 在一些实施例中,该方法还包括:

[0229] 确定熵值大于或者等于设定阈值,则获取除加密行为信息之外的其他行为信息;

[0230] 基于其他行为信息和行为识别模型,生成检测结果,检测结果用于表征行为信息是否为攻击行为。

[0231] 这里,在确定熵值大于或者等于设定阈值时,可能还存在正常的加密行为,为了提升动态检测的检测能力,本申请实施例通过构建行为识别模型,对其他行为信息进行检测,生成检测结果,检测结果用于表征行为信息是否为攻击行为。

[0232] 这里,以勒索行为为例,行为模型可以基于勒索行为AI引擎,针对无文件攻击、白进程注入类攻击、添加信任区等绕过方式,实现事中阶段的勒索防护能力,客户就算被黑客攻陷,都能够在勒索载荷落地执行阶段防住,AI引擎通过对主流勒索病毒加密行为的学习、检测、打分,能够精确定位勒索攻击行为,实现自动阻断,遏制勒索蔓延。

[0233] 在相关技术中,病毒加壳、混淆、注入白进程等绕过手段层出不穷,静态防护存在能力边界,总有部分勒索病毒通过某种方式执行起来,造成用户数据损失。若在病毒执行初

始阶段,发现并阻止加密进程,能够有效保护数据进一步受损,为此提出基于行为的勒索病毒检测方案。勒索行为检测流程如图6所示,通过数据采集引擎采集用户操作系统进程调用的事先定义的API序列、进程动作序列、文件操作行为序列,威胁分析引擎基于专家知识完成可疑行为模式筛选,最终基于AI的行为模型进行训练,采用模型融合的方式,实现基于行为模型的勒索行为模式识别,在实际应用中,基于行为模型对可疑行为模式(删除文件、加密文件、删除卷影、修改注册表、请求勒索链接)进行判断,勒索行为的高精度识别。

[0234] 示例性地,参照图7,图7为神经网络提取行为模型示意图,进行动态行为监测,根据API序列、进程动作、文件操作等原始数据构建行为图,行为图有助于发现不同行为之间存在的映射关系。基于该图对行为本身、行为操作对象进行量化,形成可计算的行为向量,而行为作为一种序列化的数据,需要具备针对长序列的处理方案,这里采用时序网络对长序列进行Embedding(嵌入),进一步地完成行为向量压缩与行为特征提取。至此获得了已采集数据的特征向量,后续结合贝叶斯分类、SVM、决策树等多个模型完成最终的分类任务。基于多粒度特征的行为引擎是利用自动化采集的行为日志、手动构建的多粒度行为特征来提高决策树分类器性能的方法。实现的步骤为:

[0235] 收集行为日志:通过自动化方式收集进程的行为日志,包括执行期间的系统事件序列以及相应的参数。这些日志数据可以提供关于进程行为的详细信息。

[0236] 构建行为图:将日志中的行为操作转换为二部行为图。图包含两种类型的顶点:事件操作和参数。在每个行为操作和参数之间绘制边缘,以图的形式表示能够更好地提取特定的行为模式(例如网络通信、文件加密修改等)。

[0237] 编码行为模式(Embedding):将每个行为模式压缩为稀疏的One-hot(一位有效编码向量)向量。该二维向量表示每个进程是否包含特定的操作或参数。进一步通过神经网络将其转换为模式嵌入的紧凑表示。有助于学习到更复杂的特征表示,提高勒索软件分类器的性能。

[0238] 结合专家知识:将自动化收集的行为嵌入与专家系统的多粒度行为特征进行拼接,将特征融合作为决策树分类器的最终输入。

[0239] 训练决策树模型:使用收集到的数据和特征,训练一个决策树分类器,判断进程是否为勒索软件。决策树分类器可以根据输入的特征向量,自动选择最佳路径来进行分类

[0240] 在一些实施例中,该方法还包括:

[0241] 响应于指示信息,阻断当前进程;

[0242] 确定将当前文件同步至目标文件完成,则基于目标文件,生成一键回滚操作指令;

[0243] 响应于一键回滚操作指令,对当前文件进行回滚操作,以将当前文件恢复至目标文件。

[0244] 这里,响应于指示信息,本申请实施例在触发备份方案的同时,实现智能阻断和反制措施,对当前进程进行阻断,并且恢复相关文件,在保护文件恢复操作便利性的同时,也提升了对恶意文件的安全防护能力。

[0245] 示例性地,文件被加密时,文件熵(描述混乱程度)会显著增加,利用该特征为显著特点,文件熵显著增加时自动启动内存备份功能,如果发现文件被加密,则阻断加密进程,并且从内存中恢复相关文件。

[0246] 在恢复文件的过程中,本申请实施例支持一键回滚,一键回滚是指在备份数据时,

系统会自动记录当前数据的状态,并将其保存在备份文件中。当需要回滚时,用户只需点击一键回滚按钮,系统便会自动将备份文件中的数据恢复到之前的状态,从而实现数据的快速恢复。其便利性在于,用户无需手动查找备份文件,也无需手动恢复数据,只需简单地点击一键回滚按钮即可完成整个恢复过程,大大提高了数据恢复的效率和便利性。

[0247] 在一些实施例中,反制措施还包括事件定性与故事线构建,对攻击行为等安全事件进行分类和分析,并将它们组织成一个完整的故事线,以便更好地理解和应对安全威胁。这种方法可以帮助安全团队更快地识别和响应安全事件,从而减少潜在的损失和风险。

[0248] 在一些实施例中,RDP远程暴破登录是目前黑客攻击的常用手段之一,而企业运维管理人员常因为服务器众多,为方便管理运维而使用安全性较低的登录密码,极容易爆破而导致被勒索。

[0249] 在本申请实施例中,考虑服务器远程登录的多因素认证技术,通过监听RDP会话消息,当检测到有新会话接入时,自动切换到二次认证桌面,该桌面只有二次密码验证的窗口,仅允许输入密码验证,禁止其他操作。也支持仅允许指定IP或网段的主机访问服务器,实现服务器远程登录的统一认证管理。

[0250] 在一些实施例中,当攻击者进入被攻击终端后,为绕过终端防护软件中的静态检测,通常尝试卸载终端防护软件,从而达到病毒落盘执行的目的。为了缓解该类情况导致的恶意病毒执行,设计二次认证方案,通过在控制端设置防退出/防卸载密码,并下发到用户代理(Agent)终端,当用户尝试退出、卸载终端防护软件时,需要输入该密码,否则不能进行退出、卸载操作。

[0251] 下面,结合一应用示例对本申请实施例进行详细说明。

[0252] 当前勒索攻击防护技术方案,以规则防护为主,并没有广泛应用AI技术。类似的,动态防护(执行阶段行为分析)各厂商实现路径也有所不同,包括云端基于规则的主防方案、终端基于规则的进程高可疑行为分析方、端云联动基于AI的行为AI防护引擎等;然而,国内厂商静态引擎、动态引擎大多孤立存在,分别用于闭环恶意载荷落地阶段防护与执行阶段防护,并没有把终端静态-动态引擎做很好的协同。

[0253] 为缓解上述问题,本应用示例从勒索病毒静态检测、动态行为检测、防绕过、勒索处置等多个方面,通过分析数十种热门勒索家族样本,挖掘勒索病毒在入侵、绕过、加密、传播等不同攻击场景采用的技术手段,针对性的提出检测与防护方案,能够有效的发现并阻断勒索病毒的执行与传播。

[0254] 本申请实施例提供了一种勒索攻击智能识别与风险响应方案。如图8所示,图8为本应用示例的勒索攻击智能识别与风险响应的系统架构图。该系统是一种面向未知勒索攻击的智能识别与响应技术,以人工智能技术为核心,形成基于AI的勒索攻击防护系统,通过面向勒索行为的精准识别、双重/多重勒索攻击阻断技术、勒索软件破解技术、勒索攻击备份技术上达成核心突破,实现勒索病毒软件感知、分析、识别、响应一体化。参照图8,该架构主要包括4项核心子系统:

[0255] 子任务1:勒索行为特征库与攻击识别模型子系统。

[0256] 勒索行为特征库与攻击识别模型子系统,致力于建设勒索行为特征库,与攻击识别模型的训练迭代系统,训练勒索人工智能防御模型,形成面向未知勒索攻击的防护方法与手段;具体的,通过活跃样本收集、工业互联网环境构建和沙箱运行,进行勒索样本特征

分析(二进制反汇编+沙箱动态分析),从而形成勒索攻击行为特征库(勒索攻击通用特征库+工业互联网勒索攻击专用特征库);进而借助AI模型训练平台,训练勒索人工智能防御模型,形成面向未知勒索攻击的防护方法与手段。

[0257] 子任务2:勒索攻击精准识别与多重勒索防御子系统。

[0258] 勒索攻击精准识别与多重勒索防护子系统,致力于开发互联网企业数据勒索攻击智能识别与响应系统,实现工业互联网中勒索攻击高精准、近自动化防护,同时避免多重勒索下的数据窃取;具体的,任务构成包括数据采集模块、动静结合智能防御模块、勒索处置与响应模块,在以下部分构建核心技术壁垒:

[0259] 国内领先的静态AI检测、定性引擎,实现广撒网勒索病毒攻击的低成本防护与定性;国内首创系统化构建基于诱饵系统的指标体系,针对关键设备、阶段进行指标采集,上收端侧威胁数据,联结各攻击阶段威胁感知AI输出攻击场景,达到对威胁(勒索、窃密等)高自动化防护的效果;同时形成不少于4种轻量级加密技术,覆盖研发设计、生产制造、运行维护等不少于6种重要数据类型;

[0260] 首创多层轻量备份技术,综合动态实时备份(基于动态AI)、增量快照备份(基于windows VSS),结合存储备份,形成对客户数据全面无死角保障;

[0261] 完备的处置响应技术,通过端点较为全面的数据遥测能力与端点完整的故事线与进程链还原能力,结合安全专家案例与安全运维,实现响应处置精准性;预计将建立勒索软件破解资源池涵盖60种以上破解脚本。

[0262] 子任务3:勒索攻击轻量备份与数据恢复子系统。

[0263] 该部分由三大模块构成,分别是:动态实时备份模块、增量快照备份模块和勒索数据恢复模块;其中,动态实时备份模块,通过子系统2处置响应模块中轻量备份机制对于疑似勒索进程的判定,实现在疑似勒索进程执行阶段加密文件的实时备份恢复。增量快照备份模块,通过基于VSS(Windows Virtual Shadow Copy Service)的增量快照备份组件,以及勒索软件删除卷影防护组件,实现针对操作系统定时快照、增量备份,允许用户在遭遇勒索攻击时实现对系统的一键回滚,起到数据保护的轻量兜底功能。

[0264] 子任务4:勒索软件破解子系统。

[0265] 突破已知勒索软件逻辑漏洞,结合DES、AES等国际主流加密算法特征,建立勒索软件破解资源池;具体的,该子系统中将基于软件逆向与加密算法分析的勒索攻击漏洞协议破解技术,通过分析热门勒索软件加密模式,确认勒索病毒采用的加密方案,结合勒索软件漏洞、二进制逆向分析、穷举恢复、共模破解等技术,挖掘勒索病毒解密密钥,形成破解方案;继而将破解的软件形成解密脚本与工具,形成勒索攻击漏洞协议破解技术资源池,并实现云端部署、用户高效访问。

[0266] 本应用示例采用人机共智理念对抗勒索病毒的理念进行勒索行为的智能识别与响应。参照图9,图9为采用人机共智理念对抗勒索病毒的流程示意图。其具体分为:

[0267] (1)预防。

[0268] 1、在前期开展勒索风险的评估,及时发现可能存在的安全隐患;2、通过安全加固借助产品的专有安全能力:加强网络防护,提升终端安全基线,减少终端端口开放、弱口令、漏洞等安全风险点,防止被RDP爆破、漏洞利用、U盘传播、钓鱼邮件等方式感染病毒。3、在终端层面利用杀毒软件快速查杀各种类型勒索病毒,防止数据被加密。

[0269] (2)监测。

[0270] 勒索病毒入侵后会横向扫描、广泛扩散繁殖,需要实时监测终端恶意文件、终端可疑操作等异常行为,通过多种手段(诱饵、加密行为检测)监测勒索病毒执行活动,在数据被加密之前或加密过程中及时发现勒索病毒。

[0271] (3)处置。

[0272] 对勒索病毒进行集中处置,同时进一步分析造成安全事件的原因,快速采取措施进行根除,尽快恢复业务正常运转。并提前储备应急资源针对关键敏感数据实施数据联动备份,将损失减低到最小。

[0273] 下面分别对子系统2、子系统3和子系统4进行详细说明。

[0274] 一、对子系统2进行详细说明。

[0275] 参照图8,子系统2包括:数据采集模块、动静结合智能防御模块和勒索处置与响应模块。

[0276] (1)数据采集模块。

[0277] 数据采集是指收集和记录图8系统所监控的终端设备上的安全事件和活动,用于监控和响应网络终端设备上的安全事件。主要包含采集信息爆破攻击事件、文件落地、注册表项、命令执行、进程API、文件追踪、资源占用、网络行为等。

[0278] 其主要来自终端上采集的二进制内容(文件、网络流量、内存快照等)、日志(WindowsEventLog、防火墙日志、Web日志等)、事件和监控记录(进程行为、账户活动等),它们被采集、存储、分析和处理,用于作为原始输入,实现终端安全的各类检测和防护方案。主要采用两种技术方案:

[0279] 内核态实时监控:该技术通过内核消息订阅、MiniFilter、WFP等来实现进程行为的实时监控。

[0280] 优点:监控点单一(无需在用户态影响应用程序);单个事件覆盖率最高;可在内核态过滤,提高事件处理性能;可同步监控,进行拦截防护;可对用户态的对抗免疫。

[0281] 用户态HOOK:该技术通过将监控代码注入到应用程序中,以API调用为监控点。

[0282] 优点:一些事件只能通过该技术采集;上层事件信息比较完整详细;可做效果和性能之间的灵活平衡;可同步监控进行拦截防护。

[0283] (2)动静结合智能防御模块。其包括:1恶意软件/流量静态分析系统和2恶意行为动态识别系统。

[0284] 1.恶意软件/流量静态分析系统包括:勒索病毒静态特征匹配模块和文件/流量提取模块。

[0285] 第一:勒索病毒静态特征匹配模块。下面,对勒索病毒静态特征匹配模块进行详细说明。

[0286] 传统的静态病毒检测方法主要有MD5(Message-Digest Algorithm 5,消息摘要算法第五版)、病毒特征码和规则匹配这三大类。这些传统技术本质上都是对文件的字节信息进行匹配,这导致他们通常无法检测新变种、新家族等未知威胁。下面以勒索病毒样本GandCrab5.0.0为例讲解几种传统技术方案的思想和缺点。

[0287] (1)MD5是匹配样本文件的整体MD5哈希值,也就是需要完全匹配病毒文件的二进制序列,改变一个字节都不行。

[0288] (2)病毒特征码是匹配文件内容中的特定二进制串(被称为“特征码”),通常是匹配病毒的恶意代码部分,比如需要匹配图1中完整的ABC代码片段。

[0289] (3)规则匹配比起特征码更灵活一些,是匹配多个二进制串的组合,它支持匹配一条正则表达式描述的规则,例如“当A出现,且B或C有一个出现”,对应正则规则A&(B|C)。

[0290] 沙箱是一种动态检测技术,他通过模拟运行病毒文件,捕获病毒的动态可疑行为,举证比较说服力。但其显著缺点是资源开销巨大,因此沙箱通常部署在云端或终端,较少部署在网关设备。基于性能考虑,一般把沙箱接在静态检测引擎之后(这些高性能引擎可能是基于MD5、特征码、规则或者AI)。这样只有极少的可疑文件需要交给沙箱判定。

[0291] 参照图10,图10为GandCrab的代码片段示意图。上述几类传统静态病毒检测方案虽然技术原理和检测能力各有不同,但它们的检测对象本质上都是字节信息。该共性也成为他们的共同缺陷。此类字节信息属于原始的、低层特征,其在病毒演化和逃避检测的过程中通常是脆弱多变的。比如,当勒索病毒GandCrab演化到变种5.0.3时,其代码片段变成了DBC(如图10中(b))。上述传统的静态检测方法此时全部失效,失效原因分别是:MD5发生变化,特征码变化,规则匹配不上。因此传统方法通常无法检测新变种、新家族等未知威胁。正是由于传统方法的这些缺陷,SAVE提出了使用机器学习技术去检测未知病毒或新变种。

[0292] 不同病毒变种间的底层二进制代码片段在不断变换。为了识别未知病毒威胁,不再依赖于前述传统方法依赖的字节级特征,而是使用AI技术提取稳定、可靠的高层次特征。当病毒变种间为了实现相似乃至相同的病毒功能,他们代码的高层次语义特征往往是相似的(如图10中的(a)和图10中的(b)所示)。正是基于对病毒演化本质的深入理解,通过神经网络等多种机器学习算法自动提取高层次特征。

[0293] 参照图11,图11为基于神经网络识别未知病毒的原理示意图。深度神经网络是由多层的非线性神经元构成的网络计算模型,它模拟了生物神经系统的链接方式,能够在系统中有效、快速的传递有效信息(如图11所示)。深度神经网络的强大之处在于:通过学习海量的正常文件样本和病毒文件样本,它能自动地、逐层地凝练更高层次的特征。比如说,信息在网络传递的过程中,其表征的含义从最开始输入的文件字节特征0xa21d(识别一个字节),逐渐进化到语句特征 (识别一个指令),函数特征“func()”(识别一个函数)和语义特征“加密操作”(识别一个操作/行为,比如勒索病毒通常具有的加密操作),最后完全自动化的构建出稳定可靠的高层次病毒特征。实际中,取决于网络结构和深度的不同,信息演化的路径不尽相同,但大体上是沿着这样的方式。比起只利用字节特征的传统方案形成明显优势,具有很强的泛化能力。能够更好的识别未曾见过的病毒样本,抵御抗病毒变种和新病毒家族等未知威胁。

[0294] 参照图12,图12为人工智能检测引擎基本原理的示意图。

[0295] 图12描述了AI检测引擎基本原理。以PE文件查杀为例,AI检测引擎会从文件的头(文件头)、文件节、资源和签名(证书)等多个部分提取信息,作为判别输入。对于原始二进制文件,通过多种方法(词向量嵌入,主成分分析,深度神经网络等)提取出信息量丰富、类间界限明显,稳定可靠的的高层次向量化特征(特征向量)。基于特征向量,AI检测引擎利用集成学习,综合多种分类算法(随机森林,神经网络,支持向量机SVM等)进行鉴定。最后,综合评分系统整合各模型检测结果,综合判断文件黑白属性。

[0296] 除了使用AI技术大幅提升检测能力,还在云端通过生成对抗网络(GAN)的思想(如

图13,图13为对抗网络学习模型的示意图),采用“左右互搏”的方式持续学习,参照图13,增强模型健壮性和检测能力。一方面,GAN框架中的“病毒生成器(Generator)”模块能够模拟病毒变种的制作过程,不断生成新的病毒变种文件,以逃逸当前版本引擎的检测。这些病毒文件将为AI检测引擎持续提供模拟未知威胁的训练数据,促使AI检测引擎不断加强对未知威胁的检测能力。另一方面,AI检测引擎的SAVE(Classifier,分类器)输出检测结果也会反馈给“生成器”,促使其生成更有威胁的病毒文件。通过两个模块的循环促进,提升AI检测引擎的检测能力。

[0297] 参照图14,图14为多智能体模型推荐架构示意图,病毒变种千变万化,仅实现已知病毒检测能力,在实际应用中不足以满足客户对终端安全的保障需求。基于这一目的,引入多智能体模型推荐架构增强未知病毒的检测能力,通过对AI模型(随机森林和神经网络)的深度和层级的加深,对输入的特征向量进行鉴定,输出多分类结果,增强了AI模型泛化性和检出精度。同时,多智能体模型推荐架构不仅依赖于原有提取的通用性特征,同时新增AI技术对罕见性特征进行深度提取,获得更为稳定、可靠的高层次特征。能够更好的识别未曾见过的病毒样本,抵御新型抗病毒变种和新病毒家族等未知病毒。

[0298] 2.恶意行为动态识别系统。

[0299] 勒索病毒由于攻击门槛逐渐降低、攻击入口增加导致勒索病毒变种发展迅猛,这非常考验终端防护产品对未知勒索威胁的检测能力。这里对勒索病毒检测能力进行全新升级,引入多智能体模型推荐架构增加AI泛化能力,对可疑文件进行多重AI检测,提升对未知威胁的检测能力,同时对判黑的威胁文件通过可拔插式AI判别是否为勒索病毒。可以清楚的告知客户帮其防住了勒索病毒,提升客户感知。通过对抗性AI训练,该AI架构对勒索的精准率可提升到99%以上。用户可直观地掌握内网终端是否中了勒索病毒,影响范围有多大,快速采取响应措施。

[0300] 勒索病毒在入侵主机会进行横向传播扩散,影响范围十分广泛,一台终端中毒,全网业务瘫痪。为监控异常文件操作,通过在系统关键目录,放置诱饵文件,并且保证这些诱饵文件会被优先枚举到,当有勒索程序对诱饵文件进行修改或删除时,将触发驱动拦截该进程行为,并将该进程信息上报给应用层进行病毒文件查杀。针对性的勒索诱捕方案,主动进行勒索病毒的防御,及时阻止勒索病毒的大范围传播,全面阻止业务不可逆终端,保护主机安全。

[0301] “勒索行为AI引擎”能够针对无文件攻击、白进程注入类攻击、添加信任区等绕过方式,实现事中阶段的勒索防护能力,客户就算被黑客攻陷,都能够在勒索载荷落地执行阶段防住,AI引擎通过对主流勒索病毒加密行为的学习、检测、打分,能够精确定位勒索攻击行为,实现自动阻断,遏制勒索蔓延。

[0302] 病毒加壳、混淆、注入白进程等绕过手段层出不穷,静态防护存在能力边界,总有部分勒索病毒通过某种方式执行起来,造成用户数据损失。若在病毒执行初始阶段,发现并阻止加密进程,能够有效保护数据进一步受损,为此提出基于行为的勒索病毒检测方案。通过采集用户操作系统进程调用的API序列、进程动作序列、文件操作行为序列,并基于专家知识完成可疑行为模式筛选,最终采用模型融合的方式,实现勒索行为的高精度识别。勒索行为检测流程如图6所示和神经网络模型的生成,如图7所示。并基于其构建的行为模型进行动态检测。

[0303] 本应用示例提供的系统还可以采用机器学习的检测框架进行攻击行为的检测,使用GBDT(Gradient Boosting Decision Tree)算法用于攻击检测过程,结合了决策树和梯度提升两种模型的优点,构建勒索软件的分类器。基于集成学习Boosting的思想,将弱学习器组合成一个强学习器。决策树由结点和有向边组成,在进行良性软件与勒索软件分类时,其中内部结点表示勒索病毒样本的特征,叶子结点表示软件类别。通过递归选择最优特征,分割训练数据,递归直至到达叶子结点,即为其所属类别。GBDT方法的核心思想在于利用梯度下降法近似求解每一颗决策树,具体来说,就是在每次迭代中,使新建的决策树都沿负梯度方向减少损失函数。

[0304] 二、下面对子系统3进行详细说明。

[0305] 参照图15,勒索攻击备份与数据恢复子系统主体框架如图15所示,主要包括勒索数据恢复、策略管理层、动态实时备份、I/O系统层、增量快照备份、产品自身防御层、备份区、等模块,共同构建勒索攻击场景下客户侧重要数据的高效备份与快速恢复能力。下面针对备份技术的研究现状以及勒索备份与恢复技术的核心能力(动态实时备份、增量快照备份、勒索数据恢复)进行展开描述。

[0306] 在本应用示例中,勒索备份整体方案分为三大类:实时动态备份、增量快照备份、全量存储备份;

[0307] 实时动态备份,主要在勒索执行阶段,通过对勒索可疑行为识别(如:通过熵值计算发现勒索对象),在对应终端触发阶段进行实时动态数据进行快速临时备份;具体实现上,为保障备份的实时性,通常通过小文件备份、大文件防护方案进行;备份完成之后进行本地存储,若确定为勒索攻击则进行一键回滚;若判定过后认为并非勒索攻击,则放弃备份内容。

[0308] 以当前文件为例,若确定当前文件为小文件,则对小文件进行动态实时备份。

[0309] 参照图16,图16为勒索实时动态备份方案,其具体的步骤包括如下:

[0310] 1、勒索软件试图加密文件;

[0311] 2、加密请求被截获,基于勒索软件缓解策略,判断其恶意更改的可能性。

[0312] 当一个加密请求(request)被安全系统或某种机制捕获并分析时,会运用特定的算法来计算和评估,例如:勒索软件缓解策略,确定该加密请求是否包含潜在的恶意修改(malicious change),即分析该请求是否有意进行非法操作或篡改数据的风险概率。

[0313] 3、如果其恶意更改的可能性概率较高,则在内存(in-memory)中创建备份。

[0314] 4、加密请求被恢复执行,对文件进行加密。

[0315] 当基于上述的勒索软件缓解策略确定该加密请求(request)的安全性后,如果确定该请求可以继续执行(resume),接下来的操作可能是对目标文件,例如图中的文件1,进行加密处理。这样,即使请求后续涉及了文件操作,由于文件已被加密,也能确保数据在传输或处理过程中的安全。

[0316] 5、使用内存中的副本恢复原始文件。

[0317] 在相应的场景下,当恶意更改的可能性概率较高,检测是恶意更改或异常操作时,可以通过之前创建的内存中备份(in-memory copy)来恢复原始文件。这样即使原始文件遭到破坏或加密,也能基于安全存储在内存中的临时备份数据进行快速恢复。

[0318] 将勒索缓解环节引入备份恢复作为兜底方案,在遭遇疑似勒索时,主动在内存中

对文件1进行实时备份;如果没有被加密,则自动删除;如果被加密,则从内存中进行恢复;加密判定方面,文件被加密时,文件熵(描述混乱程度)会显著增加,利用该特征为显著特点,文件熵显著增加时自动启动内存备份功能,如果发现文件被加密,则阻断加密进程,并且从内存中恢复相关文件。

[0319] 增量快照备份,核心思路是针对系统磁盘快照,在定期保存快照,及增量修改部分构成的备份卷影;如果发生勒索,则根据用户配置,实现自动恢复到某一节点的备份卷影,或者根据备份卷影内容,定向恢复某些文件。快照卷影备份经常使用的方式是windows系统自带的卷影复制服务(Volume Shadow Copy Service,VSS),其基本架构如图17(图17为快照卷影备份的基本架构示意图),其架构具体包括:

[0320] 1)Requestor(请求程序):

[0321] 请求程序是一个负责执行以下任务的软件(这个可以理解为实现备份应用程序的控制端):

[0322] 1、启动VSS备份请求

[0323] 2、处理来自Writer的备份指令,包括选择哪些文件进行备份以及应使用哪种方法备份这些文件。

[0324] 3、将卷影副本数据备份到介质。

[0325] 4、从磁盘删除卷影副本数据以指示备份完成。

[0326] 2)Writer(写入器)和组件:

[0327] 卷影副本保证数据一致性的技术关键是Writer和它们的组件。

[0328] Writer:应用程序或服务的组成部分,与VSS配合使用,使应用程序的数据在卷影副本备份请求时保持一致状态。

[0329] 组件:一组选定要备份的文件或文件夹,由Writer控制下的应用程序或服务来控制。例如:微软自家产品Hyper-V、SQLServer等都实现了writer。

[0330] 特别注意的是,Writer和它们的组件本质上是为了解决业务系统在备份过程中内存与快照之间的数据不一致问题,真正备份数据的不是它。

[0331] 3)Providers(提供程序):

[0332] 提供程序负责管理卷影副本备份中所涉及的卷,并创建卷影副本。提供程序与操作系统(基于软件)或磁盘阵列(基于硬件)上的卷影副本创建功能交互作用。

[0333] Providers结合Requestor的备份策略组合起来有两种备份方式:

[0334] 1.基于硬件提供者(Hardware Provider)以实现完整副本拷贝。

[0335] 2.基于系统提供者(System Provider)或软件提供者(Software Provider)实现写入时复制(只能在本机工作),且这种机制的备份单位非常小,举例来说几GB的文件如果实际磁盘扇区没有被复写,是不会产生额外的备份空间的。

[0336] 参照图18,图18为基于硬件提供者(Hardware Provider)以实现完整副本拷贝的流程示意图。

[0337] 步骤1801:请求程序(Requestor)要求卷影复制服务枚举编写程序,收集编写程序元数据,并准备创建卷影副本。

[0338] 每个编写程序(Writer)都会为需要备份的组件和数据存储创建XML描述,并将其提供给卷影复制服务VSS。编写器还定义了用于所有组件的还原方法。卷影复制服务向请求

程序提供编写程序的描述,而请求程序则选择要备份的组件。

[0339] 卷影复制服务通知所有编写程序准备数据以进行卷影复制。

[0340] 每个编写程序都会根据需要准备数据,例如完成所有未结束事务、滚动事务日志和刷新缓存。当数据准备好进行卷影复制时,编写程序将通知卷影复制服务。

[0341] 卷影复制服务通知编写程序将应用程序写入I/O请求暂时冻结几秒钟(仍然可以执行读取I/O请求),创建卷的卷影副本需要这几秒的时间。应用程序冻结的时间不允许超过60秒。卷影复制服务刷新文件系统缓冲区,然后冻结文件系统,从而确保正确记录文件系统元数据,并以一致的顺序写入要进行卷影复制的数据。

[0342] 卷影复制服务通知提供程序创建卷影副本。卷影副本创建周期不超过10秒,在此期间,对文件系统的所有写入I/O请求都将保持冻结状态。

[0343] 步骤1802:VSS Coordinator与Writers交互,通知它们将要创建卷影副本并要求其做好数据一致性准备工作。

[0344] 步骤1803:硬件Provider(如存储阵列控制器)收到通知后,开始对即将进行快照操作的LUN(逻辑单元号)进行相应准备。

[0345] 步骤1804:快照创建完成后,硬件Provider通知VSS已成功创建了卷影副本,并返回新快照的相关信息。

[0346] 步骤1805:根据这些信息,Requestor可以开始从快照读取数据以进行备份或其他操作,而不会影响到生产环境的数据。

[0347] 步骤1806:备份任务完成后,VSS协调各个组件撤销之前所做的临时更改(如果有),并将系统状态恢复至正常工作模式。

[0348] 步骤1807:VSS通知编写程序解除冻结应用程序写入I/O请求。此时,卷影复制服务释放文件系统写入I/O请求。应用程序可以继续将数据写入正在进行卷影复制的磁盘。请求程序可以重试该过程(返回步骤1801)或通知管理员稍后重试。

[0349] 这里,如果已成功创建卷影副本,则卷影复制服务会将卷影副本的位置信息返回给请求程序。在某些情况下,卷影副本可以临时作为读写卷使用,以便VSS和一个或多个应用程序可以在卷影副本完成之前,更改卷影副本的内容。VSS和应用程序进行更改后,卷影副本将变为只读。此阶段称为自动恢复,用于撤消卷影副本卷上在创建卷影副本之前未完成的任何文件系统或应用程序事务。

[0350] 第三种备份方案为外部存储备份机制,通过将业务数据转存在其他存储空间的方式来保留一份完整的业务数据,当业务数据出现故障时可通过备份数据进行恢复。备份可以独立存在,不依赖于原存储数据,但由于是完整数据拷贝所以需要一定时间;具体又分为本地备份、云备份、离线备份等多种方案。此类备份通常遵循3-2-1原则,即:3重备份(3份备份,最大程度上避免备份失效等),2地存储(在两个不同的区域,以防自然灾害等对数据中心带来的物理灭失),1份离线备份(网络攻击兜底,通过离线存储防护接近所有网络攻击),以保障数据实现最大程度上的安全。

[0351] 参照图19,图19为小文件动态实时备份的流程示意图。下面对动态实时备份的流程进行详细说明。

[0352] 1901:任何可疑进程(process)触发防勒索的安全检查。

[0353] 1902:获取对文件的操作行为。

[0354] 在计算机安全领域,存在针对文件的多种攻击手段,例如:勒索信和诱饵,它们在执行过程中,会对文件进行对应的操作,包括:修改、删除和重命名。

[0355] 步骤1903:对任何可疑进程的文件操作行为进行安全检查,若安全检测结果为不可信,则执行步骤1904和步骤1905,若安全检测结果为可信,可以访问,则执行步骤1906。

[0356] 步骤1904:截断当前进程。

[0357] 步骤1905:进行备份。

[0358] 步骤1906:允许对文件进行加密。

[0359] 步骤1907:对勒索行为进行安全检查时,可以基于行为模型进行判断,确定是否存在勒索行为,若是,则执行步骤1908。

[0360] 步骤1908:回滚。

[0361] 由于进行了备份,提示用户存在恢复区,由用户选择是否恢复文件,防止误报。在备份区,已经被勒索加密的文件将直接丢弃。

[0362] 本应用示例中,防勒索系统安装后,任何文件的操作均会触发防勒索的安全检查,可信应用文件操作放行,非可信应用文件操作将触发备份动作,在备份入库前,防勒索系统会检查入库数据的安全性,通过文件名、后缀名、信息熵、方差值完成文件是否被勒索加密的判断。勒索病毒加密的文件会被修改文件名、后缀名,文件的熵值和方差值会发生显著变化,基于此防勒索系统可识别被勒索加密的文件,已经被勒索加密的文件将直接丢弃,并对操作该文件的进程进行终止和隔离操作,被识别为正常的数据文件则经过重复检查后进入备份区。

[0363] 此外,勒索事中数据智能备份机制,数据智能备份机制并非是全盘备份,而是配合勒索行为AI引擎(即图19中的模型判断)经过巧妙设计按需触发,即备份基于勒索行为的判定触发,既可以实现勒索病毒的精准防范,又能备份缓解勒索行为AI引擎拦截时损失的少量文件,还能确保最小的系统资源消耗。

[0364] 参照图20,图20为基于AI的小文件备份机制的示意图。

[0365] 本应用示例考虑,由于误操作、安全策略配置不当可能导致检测、防护能力被绕过等问题,因此还需要备份恢复能力做技术兜底。在对大文件进行基于访问控制的保护之外,针对其他大量的小文件,本系统设计了基于AI的小文件备份机制。

[0366] 各文件的操作动作触发检测,基于文件过滤驱动后,移交文件,基于API、文件操作(重命名、创建、删除和修改等)完成文件加密情况判断(即加密行为识别),在可疑进程对文件进行操作之前,将正常文件进行备份,基于数据块、哈希值对文件在备份区去存在情况进行检查,重复文件直接丢弃;备份区数据可随时还原用以支撑业务快速恢复。若行为AI引擎检测勒索加密行为,则并将相关进程阻断、隔离基于AI的小文件备份利用智能算法和行为分析来快速检测勒索软件、实时监测和预测异常行为、自动备份和恢复受影响的文件,提供智能阻断和反制措施,从而有效防御勒索软件的攻击并保护小文件的安全性和完整性。本方案的主要技术贡献包括以下几点:

[0367] 1、基于AI的智能备份:勒索备份机制基于勒索AI引擎,对勒索行为实现智能化、高准确、低误报识别,确保备份模块按需启动,完美结合可用性与安全性,大幅降低终端勒索备份复杂性。

[0368] 2、多层防护,精准检测:勒索行为检测以勒索行为AI引擎为基础,在国内居于领先

地位,而勒索备份机制以勒索行为检测为核心,通过未知勒索病毒静态检测,勒索诱饵防护,黑客工具防护,内存扫描防护,无文件攻击防护以及远程登录防护在事前对终端进行整体防护;在事中通过动态引擎对勒索行为进行检测与防护,并且以检测结果为基础,通过小文件实时备份与关键目录隔离防护对小微文件与关键的业务目录进行备份与勒索防御;在事后通过终端一键回滚完成对被加密文件的回滚与恢复;形成多层次,高精准防护机制,实现对客户终端环境的全面防护。

[0369] 3、低成本,省心可靠:对文件实现精准按需备份,静态增量快照减少终端占用资源,进而降低用户办公感知,对客户日常业务不造成影响;并且将所有备份存储在终端本地,不增加外部存储从而大幅降低成本。

[0370] 5、防御闭环,一键回滚:对勒索行为事件,通过智能检测,主动防御,一键回滚形成终端防勒索闭环,大幅降低终端勒索风险。

[0371] 本方案中基于AI的小文件备份在防御勒索软件方面具有重要意义,主要包括以下几点:

[0372] 1、快速检测勒索软件:AI技术可以通过分析文件的特征和行为模式来快速检测和识别潜在的勒索软件。AI算法可以学习和识别勒索软件的特征,从而在早期阶段发现并阻止勒索软件的攻击。

[0373] 2、实时监测和预测:基于AI的小文件备份可以实时监测文件的变化和活动,识别异常行为并发出警报。AI算法可以通过监测文件的读写操作、文件属性的变化以及未经授权的文件访问等,实时预测和识别可能的勒索软件攻击行为。

[0374] 3、自动备份和恢复:基于AI的小文件备份系统可以自动进行定期备份,并通过智能算法识别重要文件和数据。一旦发现勒索软件攻击,备份系统可以自动恢复受影响的文件到其正常状态,从而快速恢复被加密或损坏的文件。

[0375] 4、异常检测和行为分析:AI技术可以分析文件和用户行为的模式,识别异常活动并采取相应的措施,可以检测到未经授权的加密行为或大规模文件变动,从而及时发现勒索软件攻击。

[0376] 智能阻断和反制措施:基于AI的小文件备份系统可以根据检测到的勒索软件行为自动采取智能的阻断和反制措施,以遏制勒索软件的传播和影响范围。

[0377] 若确定为大文件,则执行基于访问控制的大文件保护。访问控制的具体参见前述访问控制的相关内容。因此,本系统所设计的基于访问控制的大文件保护对防御勒索软件具有重要的意义。通过限制未经授权的访问、限制权限滥用、及时发现异常行为、实施数据备份和保护敏感数据,可以有效减少勒索软件对大型文件的威胁,并保护组织的数据和业务免受勒索软件攻击的影响。

[0378] 本应用示例,针对大文件和小文件都进行定时增量备份。其包括:基于VSS的增量快照备份和勒索软件删除卷影防护。卷影副本创建过程主要包括以下步骤:

[0379] 1.VSS Writer通知VSS Provider开始创建卷影副本。

[0380] 2.VSS Provider冻结文件系统和应用程序写入操作,以确保卷影副本的一致性。

[0381] 3.VSS Provider创建卷影副本,并解冻文件系统和应用程序。

[0382] 4.卷影副本提供给备份软件进行备份操作。

[0383] 卷影副本恢复过程主要包括以下步骤:

[0384] 1.VSS Provider通过加载卷影副本将其恢复到原始卷。

[0385] 2.文件系统和应用程序重新连接到恢复的卷。

[0386] 3.数据恢复完成,系统恢复到正常运行状态。

[0387] Windows卷影复制服务提供了许多关键功能,使其成为数据备份和恢复的首选解决方案。

[0388] 1.一致性备份:VSS在创建卷影副本期间冻结文件系统和应用程序,以确保备份的数据是一致的,避免了备份数据中的数据损坏或不一致性。

[0389] 2.热备份:VSS可以在运行时创建卷影副本,而不需要停止或中断正在运行的应用程序和服务。这意味着用户可以在不影响系统运行的情况下进行备份。

[0390] 3.增量备份:VSS支持增量备份,只备份自上次备份以来更改的数据。这样可以大大减少备份所需的时间和存储空间。

[0391] 4.应用程序一致性:VSS可以与许多常见的应用程序(如数据库服务器和邮件服务器)进行集成,确保备份和恢复期间的应用程序数据一致性。

[0392] 5.多卷支持:VSS可以同时备份和恢复多个卷,为复杂的存储环境提供全面的支持。

[0393] Windows卷影复制服务在数据备份和恢复中具有许多优势,使其成为广泛采用的解决方案。

[0394] 1.节省存储空间:仅备份更改的数据,减少了备份所需的存储空间。

[0395] 2.快速恢复:通过基于增量备份的方式,恢复数据更快速,因为只需要还原最新的完整备份和应用增量更改。

[0396] 3.数据一致性:VSS确保备份数据的一致性,即使在文件被访问或修改时也能保持数据的完整性。

[0397] Windows卷影复制服务(VSS)是一项关键的数据备份和恢复服务,通过创建卷的卷影副本,提供了数据一致性和可用性的保障。VSS的工作原理、关键功能和应用优势使其成为数据备份和恢复领域的重要解决方案。通过VSS,用户可以获得一致性的备份数据,灵活的备份选项和高效的恢复能力,提高了数据的安全性和可用性。无论是个人用户还是企业组织,都可以依靠Windows卷影复制服务来满足其数据备份和恢复的需求。

[0398] 虽然VSS是一种功能强大的Windows服务,但勒索软件同样可能利用其漏洞和弱点来破坏数据备份完整性。删除VSS是一种常见的攻击方式,攻击者可以利用特权访问或恶意软件来删除已创建的VSS快照,从而破坏数据的恢复能力。常见的删除VSS的攻击方式包括:

[0399] 攻击者通过获取管理员权限或其他高权限用户的凭证,可以访问和操作VSS服务,包括删除已创建的快照。

[0400] 恶意软件可能以管理员权限运行,通过调用相关的API或命令来删除VSS快照。这可以导致数据备份不完整,使恢复变得困难或不可能。

[0401] 勒索行为备份机制在实时动态备份之外,另基于Windows系统提供的VSS(卷影复制服务)技术实现了一种全盘增量快照技术,定期对全盘文件进行增量快照保存,完成对文件备份的全盘兜底。二者结合,实现了勒索行为备份机制的多重备份管理。并且勒索行为保护机制能够对备份区以及卷影实现高级别自保护,例如:带有签名的才让访问,确保备份文件与卷影万无一失。在发生了勒索事件之后,通过对备份区文件的一键回滚,即可完成业务

文件的恢复,消弭勒索事件对客户办公业务的影响。

[0402] 终端主机数据备份与恢复系统采用双重数据去重方案,旨在提高存储的使用效率并降低存储成本。这两种数据去重方案分别是基于快照的增量备份去重和基于卷设备的索引机制。下面将详细阐述这两种方案,并展示它们在提高备份效率和降低资源消耗方面的优势。

[0403] 快照技术已经超越了简单的数据保护范畴,可以用快照进行高效且无风险的应用软件测试。用快照数据做测试,不会对生产数据造成任何的破坏。对于数据挖掘(data mining)和电子发现(eDiscovery)应用,快照也是理想的测试数据源。在灾难恢复方面,快照是一种非常有效的方法——甚至是首选,非常适合遭到恶意软件攻击、人为误操作和数据损坏等逻辑错误发生时的数据恢复。

[0404] 大多数磁盘阵列的软件系统里都含有快照功能。基于磁盘阵列的快照与基于NAS的快照有非常相似的优点,即所有与磁盘阵列相连的计算机系统都可以使用这种标准的通用快照功能,包括物理服务器、虚拟机、台式机和笔记本电脑等等。快照的实施、操作和管理也都很简单。像NAS一样,很多磁盘阵列的快照功能也可以被Windows VSS、备份服务器和备份Agent等软件直接调用。一些磁盘阵列厂商还有可供非Windows平台应用系统使用的Agent代理程序。

[0405] 具体使用快照时,存储管理员可以有三种形式,即冷快照拷贝、暖快照拷贝和热快照拷贝。

[0406] (1)冷快照拷贝:进行冷快照拷贝是保证系统可以被完全恢复的最安全的方式。在进行任何大的配置变化或维护过程之前和之后,一般都需要进行冷拷贝,以保证完全的恢复原状(rollback)。冷拷贝还可以与克隆技术相结合复制整个服务器系统,以实现各种目的,如扩展、制作生产系统的复本供测试/开发之用以及向二层存储迁移。

[0407] (2)暖快照拷贝:暖快照拷贝利用服务器的挂起功能。当执行挂起行动时,程序计数器被停止,所有的活动内存都被保存在引导硬盘所在的文件系统中的一个临时文件(.vmss文件)中,并且暂停服务器应用。在这个时间点上,复制整个服务器(包括内存内容文件和所有的LUN以及相关的活动文件系统)的快照拷贝。在这个拷贝中,机器和所有的数据将被冻结在完成挂起操作时的处理点上。当快照操作完成时,服务器可以被重新启动,在挂起行动开始的点上恢复运行。应用程序和服务器过程将从同一时间点上恢复运行。从表面上看,就好像在快照活动期间按下了一个暂停键一样。对于服务器的网络客户机看来,就好像网络服务暂时中断了一下一样。对于适度加载的服务器来说,这段时间通常在30到120秒。

[0408] (3)热快照拷贝:在这种状态下,发生的所有的写操作都立即应用在一个虚拟硬盘上,系统的文件以保持高度的一致性。服务器提供让持续的虚拟硬盘处于热备份模式的工具,以通过添加REDO(重做)日志文件在硬盘子系统层上复制快照拷贝。一旦REDO日志被激活,复制包含服务器文件系统的LUN的快照是安全的。在快照操作完成后,可以发出另一个命令,这个命令将REDO日志处理提交给下面的虚拟硬盘文件。当提交活动完成时,所有的日志项都将被应用,REDO文件将被删除。在执行这个操作过程中,会出现处理速度的略微下降,不过所有的操作将继续执行。但是,在多数情况下,快照进程几乎是瞬间完成的,REDO的创建和提交之间的时间非常短。热快照操作过程从表面上看基本上察觉不到服务器速度下

降。在最差情况下,它看起来就是网络拥塞或超载的CPU可能造成的一般服务器速度下降。在最好情况下,不会出现可察觉到的影响。

[0409] 该方案的工作原理是通过Agent(代理)实时记录客户端本地被修改的数据块位置,备份时仅备份被记录的数据块。同时,增量数据也会记录在原始磁盘上的快照中。这样一来,大量未经修改的数据无需进行备份,极大减少了备份时客户端的磁盘I/O操作。此外,该方案还能释放大量的CPU资源和更多的内存资源,将对客户端业务系统性能的影响降到了最低。

[0410] 例如,对于一些大型数据库文件,在使用过程中通常只会更改其中的部分数据。基于快照的增量备份方案能够准确识别被修改的数据块位置,只备份对应的修改块,而无需将整个数据库文件进行备份。这种精确备份的方式极大地减少了备份数据的量,进而提高了备份效率,并显著降低了备份所需的存储空间。

[0411] 另一方面,终端主机数据备份与恢复系统还采用基于卷设备的索引机制。卷设备索引机制主要由索引组件和恢复组件两部分组成。索引组件负责建立和维护备份数据的索引,而恢复组件则负责根据索引进行数据恢复操作。

[0412] 1.索引组件:

[0413] 索引组件负责将备份数据的位置和相关信息存储到索引中。具体的工作过程包括:

[0414] (1)扫描备份数据:索引组件会扫描备份数据集,收集每个数据块的位置、大小和其他相关信息。

[0415] (2)建立索引:通过将数据块的唯一标识符与其位置和相关信息关联,索引组件建立一个索引表格。

[0416] (3)索引管理:索引组件会定期更新索引表格,以反映备份数据的变化情况。

[0417] 2.恢复组件:

[0418] 恢复组件负责根据索引进行数据恢复操作。具体的工作过程包括:

[0419] (1)查询索引:恢复组件首先查询索引表格,根据用户指定的恢复需求找到所需数据块的位置和相关信息。

[0420] (2)定位数据块:根据索引中记录的位置信息,恢复组件可以直接访问备份数据集,定位到所需的数据块。

[0421] (3)数据恢复:恢复组件将定位到的数据块恢复到目标设备或位置,完成数据的恢复过程。

[0422] 卷设备索引机制包括多个关键组件,确保索引的准确性和可靠性:

[0423] 1.索引表格:索引表格是索引组件的核心数据结构,用于存储备份数据的位置和相关信息。它通常采用哈希表或B+树等数据结构,提供高效的索引查询和更新操作。

[0424] 2.唯一标识符:每个数据块在索引表格中都有唯一的标识符,用于在索引查询和数据恢复过程中进行标识和匹配。

[0425] 3.元数据:索引表格中存储的相关信息包括数据块的位置、大小、时间戳以及其他关键属性。这些元数据提供了对备份数据进行管理和恢复所需的信息。

[0426] 该方案中的基于卷设备的索引机制通过索引记录了备份数据的位置和相关信息。当需要恢复特定的文件或数据时,系统可以快速定位到所需的数据块,从而提高了恢复的

效率。同时,索引机制还允许对备份数据进行增量的更新和管理,从而实现更加灵活和高效的数据恢复。

[0427] 综上,终端主机数据备份与恢复系统的双重数据去重方案(基于快照的增量备份去重和基于卷设备的索引机制)在提高存储使用效率和降低存储成本方面具有显著优势。通过精确记录和备份仅被修改的数据块,减少了备份所需的存储空间,提高了备份效率。同时,基于卷设备的索引机制保证了数据恢复的高效性和准确性。这两种方案的应用使得终端主机数据备份与恢复系统能够更好地满足组织对数据保护和业务连续性的需求。

[0428] 3.勒索数据恢复。

[0429] 本应用示例中,子系统3还包括勒索数据恢复模块。在现代信息技术环境中,数据备份和恢复对于组织的业务连续性和数据安全至关重要。为了实现持续数据保护能力(Continuous Data Protection,CDP)和满足较低的恢复点目标(Recovery Point Objective,RPO),终端主机数据备份与恢复系统采用了两种主要的数据恢复方式,即端侧自动恢复技术和云侧备份恢复技术。本方案将详细阐述这两种技术的特点和优势,并说明它们如何提供高效的数据备份和恢复能力。

[0430] 首先,端侧自动恢复技术指的是在本地设备上实现数据备份和恢复。这种技术具有以下优点:

[0431] 1.数据备份和恢复速度快:由于数据不需要通过网络传输,端侧自动恢复技术可以实现更快速的备份和恢复操作。数据可以直接从本地设备读取,减少了数据传输的延迟和网络带宽的消耗。

[0432] 2.高可靠性:端侧自动恢复技术可以在网络不稳定或无网络的情况下进行数据备份和恢复。这种情况下,端侧设备可以继续进行备份和恢复操作,不会受到网络中断的影响,具有较高的可靠性。

[0433] 云侧备份恢复技术指的是将数据备份到云端,并通过云端进行数据恢复。这种技术具有以下优点:

[0434] 1.大容量存储:云端提供了大容量的存储空间,可以满足大规模数据备份的需求。组织可以根据实际需求灵活扩展存储容量,确保备份数据的完整性和安全性。

[0435] 2.高灵活性:云侧备份恢复技术可以随时随地进行数据备份和恢复。组织可以通过云平台的用户界面或API(Application Programming Interface,应用程序编程接口)接口,方便地进行备份和恢复操作,不受地理位置和时间的限制。

[0436] 混合云备份与云存储服务、SaaS是目前最常见的两种对数据进行云备份的实现方式。其中,备份SaaS基于代替次级存储与场内软件的一种云备份方式,主要是通过对Web的应用所实现的,对其进行访问可以利用浏览器的界面来实现,但是其运行是在远程的系统中进行的,而且是被集中控制的。通常,备份SaaS的架构是被多个用户所共享的,其计价模式是边使用边付费的模式。备份SaaS的运行机理是:轻量级的代理程序在受到保护的系统上运行,数据通过程序从主站点被传输至云上。

[0437] 由于云计算的容量没有限制,可以实现离线备份,具有价格低廉的优点,因此混合云备份受到了广泛的应用。混合云备份可以把具备一定量空间的磁盘作为数据的暂时存储空间,通过高速缓存的方法把大量的数据以较快的速度发送至云中,这种备份解决方案是目前最好的数据备份方式。其运行过程为:首先以超高的速度捕捉备份信息,在磁盘上暂时

存储需要备份的数据;然后对D2D2C(Device-to-Device-to-Cloud,设备到设备到云)设备、备份软件进行加密处理,将数据传送给服务供应商;最后传输完整的备份,为了腾出存储新数据的空间,会丢弃已经很老的几乎用不到的备份数据,值得注意的是,为了保证数据恢复操作的时间,最近的数据不会被丢弃,会被保存下来。

[0438] 综上,终端主机数据备份与恢复系统中的端侧自动恢复技术和云侧备份恢复技术是两种重要的数据恢复方式。端侧自动恢复技术通过在本地设备上进行数据备份和恢复,具有快速性和高可靠性的优势;而云侧备份恢复技术通过将数据备份到云端,提供了大容量存储和高灵活性的优势。这两种技术都能实现数据备份和恢复的自动化,降低了人工干预,提高了效率。终端主机数据备份与恢复系统的采用,使得组织能够灵活、高效地保护数据,满足持续数据保护的需求。

[0439] 此外,子系统2还包括了勒索处置与响应模块。其具体包括了:

[0440] 1、一键回滚。

[0441] 备份系统支持一键回滚是指在备份数据时,系统会自动记录当前数据的状态,并将其保存在备份文件中。当需要回滚时,用户只需点击一键回滚按钮,系统便会自动将备份文件中的数据恢复到之前的状态,从而实现数据的快速恢复。这种备份系统的便利性在于,用户无需手动查找备份文件,也无需手动恢复数据,只需简单地点击一键回滚按钮即可完成整个恢复过程,大大提高了数据恢复的效率和便利性。

[0442] 2、全域响应策略下发。

[0443] 终端安全防护软件支持全域响应策略下发是指该软件可以通过集中管理平台下发安全策略,实现对所有终端设备的统一管理和控制。这种策略下发方式可以大大提高企业的安全性和效率,具有以下优势:

[0444] (1)统一管理:通过集中管理平台下发策略,可以实现对所有终端设备的统一管理和控制,避免了人工干预的繁琐和错误。

[0445] (2)实时响应:全域响应策略下发可以实现实时响应,及时发现和处理安全威胁,提高了安全性和效率。

[0446] (3)灵活性:支持全域响应策略下发的终端安全防护软件可以根据企业的实际需求进行灵活配置,满足不同场景下的安全防护需求。

[0447] (4)可扩展性:该策略下发方式可以支持大规模的终端设备,具有良好的可扩展性,适用于不同规模的企业。

[0448] (5)降低成本:通过集中管理和控制,可以降低企业的管理成本和维护成本,提高了企业的经济效益。

[0449] 在访问关系可视化中,采用统一管理的方式对终端的网络访问关系进行图形化展示,可以看到每个业务域内部各个终端的访问关系展示以及访问记录,也可以看到每个业务域之间的访问关系展示以及每个业务域的流量状态、访问趋势、流量排行,同时可以根据每个访问关系会生成访问关系控制策略,让用户决定是否启用该策略,减少了手动新增策略的工作量,提高了安全管理的效率。

[0450] 3、轻量备份机制触发。

[0451] 4、事件定性与故事线构建。

[0452] 支持事件定性与故事线构建,这意味着可以对安全事件进行分类和分析,并将它

们组织成一个完整的故事线,以便更好地理解和应对安全威胁。这种方法可以帮助安全团队更快地识别和响应安全事件,从而减少潜在的损失和风险。具备以下优势:

[0453] (1)更快的响应时间:通过事件定性和故事线构建,安全团队可以更快地识别和响应安全事件,从而减少潜在的损失和风险。

[0454] (2)更好的可视化:故事线构建可以将安全事件组织成一个完整的故事,使安全团队更好地理解安全事件的发生过程和影响。

[0455] (3)更好的决策支持:通过对安全事件进行分类和分析,安全团队可以更好地了解安全威胁的性质和来源,从而更好地制定决策和应对策略。

[0456] (4)更高的安全性:终端安全防护软件支持事件定性和故事线构建,可以帮助安全团队更好地保护终端设备和数据安全,从而提高整个组织的安全性。

[0457] 5、远程登录二次认证防护。

[0458] 参照图21,图21为RDP登录二次认证示意图,RDP远程爆破登录投毒是目前黑客攻击的常用手段之一,而企业运维管理人员常因为服务器众多,为方便管理运维而使用安全性较低的登录密码,极容易爆破而导致被勒索。

[0459] 为此设计服务器远程登录的多因素认证技术,通过监听RDP会话消息,当检测到有新会话接入时,如图21所示,1、专业黑客或团队远程登陆投毒。2、敏感时间段进行RDP远程登陆的二次密码验证。即此时自动切换到二次认证桌面,该桌面只有二次密码验证的窗口,仅允许输入密码验证,禁止其他操作。也支持仅允许指定IP或网段的主机访问服务器,实现服务器远程登录的统一认证管理。

[0460] 6、防退出/防卸载二次认证防护。

[0461] 当攻击者进入被攻击终端后,为绕过终端防护软件中的静态检测,通常尝试卸载终端防护软件,从而达到病毒落盘执行的目的。为了缓解该类情况导致的恶意病毒执行,设计二次认证方案,通过在控制端设置防退出/防卸载密码,并下发到用户Agent终端,当用户尝试退出、卸载终端防护软件时,需要输入该密码,否则不能进行退出、卸载操作。

[0462] 为了实现本申请实施例的方法,本申请实施例还提供一种安全防护装置,该安全防护装置与上述安全防护方法对应,上述安全防护方法实施例中的各步骤也完全适用于本安全防护装置实施例。

[0463] 如图22所示,该安全防护装置2200包括:第一控制模块2210和第二控制模块2220;第一控制模块2210用于若确定当前文件的存储空间数据大于或者等于设定的存储空间阈值,则生成对当前文件进行访问控制的访问控制规则,并基于访问控制规则,对当前文件进行访问控制;第二控制模块2220用于若确定当前文件的存储空间数据小于设定的存储空间阈值,则生成对当前文件进行备份的备份规则;并响应于指示信息,基于备份规则,将当前文件同步至目标文件;其中,目标文件为当前文件的备份文件,指示信息表征存在针对当前文件的攻击行为。

[0464] 在一些实施例中,安全防护装置还包括:确定模块2230和更新模块2240,确定模块2230用于若确定当前时刻为增量同步时刻,则获取当前文件的增量同步数据,增量同步数据基于当前文件的快照信息生成或者基于当前文件的增量卷影副本数据生成;更新模块2240用于基于增量同步数据,更新目标文件。

[0465] 在一些实施例中,安全防护装置还包括生成模块2250,用于基于当前文件在当前

时刻对应的数据块信息,生成增量卷影副本数据;基于增量卷影副本数据和历史索引关系,生成目标数据块的目标标识信息和增量信息,历史索引关系包括:当前文件在上一增量同步时刻对应的数据块的信息;目标数据块为数据块中的一个或多个;基于目标标识信息和增量信息,生成增量同步数据。

[0466] 在一些实施例中,备份规则包括:卷影阴影复制服务规则,第二控制模块2220还用于确定当前文件的数据在当前时刻发生变化,则暂停当前针对当前文件的写操作;基于卷影阴影复制服务规则的卷影阴影复制服务对当前文件及其所在卷的当前时刻的数据进行复制,生成卷影副本数据;确定卷影副本数据生成完成,则恢复写操作,并基于卷影副本数据,生成同步数据;将同步数据同步至目标文件。

[0467] 在一些实施例中,访问控制规则包括进程列表和映射关系,第一控制模块2210还用于确定当前进程在进程列表中,则允许当前进程访问当前文件或者获取当前进程要访问的当前文件的当前文件目录信息;确定当前进程和当前文件目录的对应关系满足映射关系,则允许当前进程访问当前文件目录,映射关系包括进程信息与文件目录的对应关系。

[0468] 在一些实施例中,访问控制规则包括一个或多个,第一控制模块2210还用于获取针对当前文件的文件访问信息,文件访问信息包括:访问用户信息、访问类型和访问等级;基于文件访问信息,确定一个或多个访问控制规则中的目标访问控制规则,其中,一个或多个访问控制规则至少包括:自主访问控制规则、强制访问控制规则和基于角色访问控制规则;基于目标访问控制规则,对当前文件进行访问控制。

[0469] 在一些实施例中,安全防护装置还包括获取模块2260,还用于获取针对当前文件的行为信息;安全防护模块还包括检测模块2270,用于对行为信息进行动态检测,若确定存在针对当前文件的攻击行为,则生成指示信息;其中,行为信息包括:加密行为信息;检测模块2270还用于基于针对当前文件的加密行为信息,确定当前文件的熵值;确定熵值大于或者等于设定的熵值阈值,确定存在针对当前文件的攻击行为。

[0470] 在一些实施例中,当前文件包括诱饵文件,检测模块2270还用于确定存在针对诱饵文件的行为,则确定存在针对当前文件的攻击行为。

[0471] 在一些实施例中,确定模块2230还用于确定熵值大于或者等于设定阈值,则获取除加密行为信息之外的其他行为信息;生成模块2250还用于基于其他行为信息和行为识别模型,生成检测结果,检测结果用于表征行为信息是否为攻击行为。

[0472] 在一些实施例中,安全防护模块还包括阻断模块2280,用于响应于指示信息,阻断当前进程;生成模块2250还用于确定将当前文件同步至目标文件完成,则基于目标文件,生成一键回滚操作指令;安全防护模块还包括恢复模块2290,还用于响应于一键回滚操作指令,对当前文件进行回滚操作,以将当前文件恢复至目标文件。

[0473] 需要说明的是:上述实施例提供的安全防护装置在进行安全防护时,仅以上述各程序模块的划分进行举例说明,实际应用中,可以根据需要而将上述处理分配由不同的程序模块完成,即将装置的内部结构划分成不同的程序模块,以完成以上描述的全部或者部分处理。另外,上述实施例提供安全防护装置与安全防护方法实施例属于同一构思,其具体实现过程详见方法实施例,这里不再赘述。

[0474] 本申请实施例还提供了一种计算机程序产品,包括计算机程序或指令,计算机程序或指令被处理器执行时实现本申请实施例公开的任一项方法的步骤。

[0475] 基于上述程序模块的硬件实现,且为了实现本申请实施例的方法,本申请实施例还提供一种电子设备。图23仅仅示出了该电子设备的示例性结构而非全部结构,根据需要可以实施图23示出的部分结构或全部结构。

[0476] 如图23所示,本申请实施例提供的电子设备2300包括:至少一个处理器2301、存储器2302、用户接口2303和至少一个网络接口2304。电子设备2300中的各个组件通过总线系统2305耦合在一起。可以理解,总线系统2305用于实现这些组件之间的连接通信。总线系统2305除包括数据总线之外,还包括电源总线、控制总线和状态信号总线。但是为了清楚说明起见,在图23中将各种总线都标为总线系统2305。

[0477] 其中,用户接口2303可以包括显示器、键盘、鼠标、轨迹球、点击轮、按键、按钮、触感板或者触摸屏等。

[0478] 本申请实施例中的存储器2302用于存储各种类型的数据以支持电子设备的操作。这些数据的示例包括:用于在电子设备上操作的任何计算机程序。

[0479] 本申请实施例揭示的安全防护方法可以应用于处理器2301中,或者由处理器2301实现。处理器2301可能是一种集成电路芯片,具有信号的处理能力。在实现过程中,安全防护方法的各步骤可以通过处理器2301中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器2301可以是通用处理器、数字信号处理器(DSP,Digital Signal Processor),或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。处理器2301可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者任何常规的处理器等。结合本申请实施例所公开的方法的步骤,可以直接体现为硬件译码处理器执行完成,或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于存储介质中,该存储介质位于存储器2302,处理器2301读取存储器2302中的信息,结合其硬件完成本申请实施例提供的安全防护方法的步骤。

[0480] 在示例性实施例中,电子设备可以被一个或多个应用专用集成电路(ASIC,Application Specific Integrated Circuit)、DSP、可编程逻辑器件(PLD,Programmable Logic Device)、复杂可编程逻辑器件(CPLD,Complex Programmable Logic Device)、现场可编程逻辑门阵列(FPGA,Field Programmable Gate Array)、通用处理器、控制器、微控制器(MCU,Micro Controller Unit)、微处理器(Microprocessor)、或者其他电子元件实现,用于执行前述方法。

[0481] 可以理解,存储器2302可以是易失性存储器或非易失性存储器,也可包括易失性和非易失性存储器两者。其中,非易失性存储器可以是只读存储器(ROM,Read Only Memory)、可编程只读存储器(PROM,Programmable Read-Only Memory)、可擦除可编程只读存储器(EPROM,Erasable Programmable Read-Only Memory)、电可擦除可编程只读存储器(EEPROM,Electrically Erasable Programmable Read-Only Memory)、磁性随机存取存储器(FRAM,ferromagnetic random access memory)、快闪存储器(Flash Memory)、磁表面存储器、光盘、或只读光盘(CD-ROM,Compact Disc Read-Only Memory);磁表面存储器可以是磁盘存储器或磁带存储器。易失性存储器可以是随机存取存储器(RAM,Random Access Memory),其用作外部高速缓存。通过示例性但不是限制性说明,许多形式的RAM可用,例如静态随机存取存储器(SRAM,Static Random Access Memory)、同步静态随机存取存储器(SSRAM,Synchronous Static Random Access Memory)、动态随机存取存储器(DRAM,

Dynamic Random Access Memory)、同步动态随机存取存储器(SDRAM,Synchronous Dynamic Random Access Memory)、双倍数据速率同步动态随机存取存储器(DDRSDRAM,Double Data Rate Synchronous Dynamic Random Access Memory)、增强型同步动态随机存取存储器(ESDRAM,Enhanced Synchronous Dynamic Random Access Memory)、同步连接动态随机存取存储器(SLDRAM,SyncLink Dynamic Random Access Memory)、直接内存总线随机存取存储器(DRRAM,Direct Rambus Random Access Memory)。本申请实施例描述的存储器旨在包括但不限于这些和任意其它适合类型的存储器。

[0482] 在示例性实施例中,本申请实施例还提供了一种存储介质,即计算机存储介质,具体可以是计算机可读存储介质,例如包括存储计算机程序的存储器2302,上述计算机程序可由电子设备的处理器2301执行,以完成本申请实施例方法的步骤。计算机可读存储介质可以是ROM、PROM、EPROM、EEPROM、Flash Memory、磁表面存储器、光盘、或CD-ROM等存储器。

[0483] 需要说明的是:“第一”、“第二”等是用于区别类似的对象,而不必用于描述特定的顺序或先后次序。

[0484] 另外,本申请实施例所记载的技术方案之间,在不冲突的情况下,可以任意组合。

[0485] 以上,仅为本申请的具体实施方式,但本申请的保护范围并不局限于此,任何熟悉本技术领域的技术人员在本申请披露的技术范围内,可轻易想到变化或替换,都应涵盖在本申请的保护范围之内。

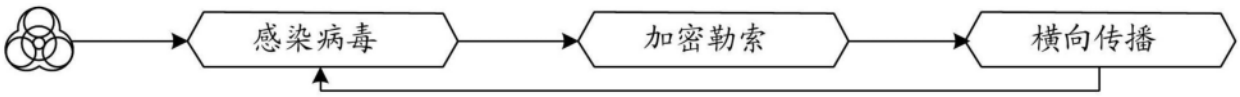

感染病毒
加密勒索
横向传播

图 1

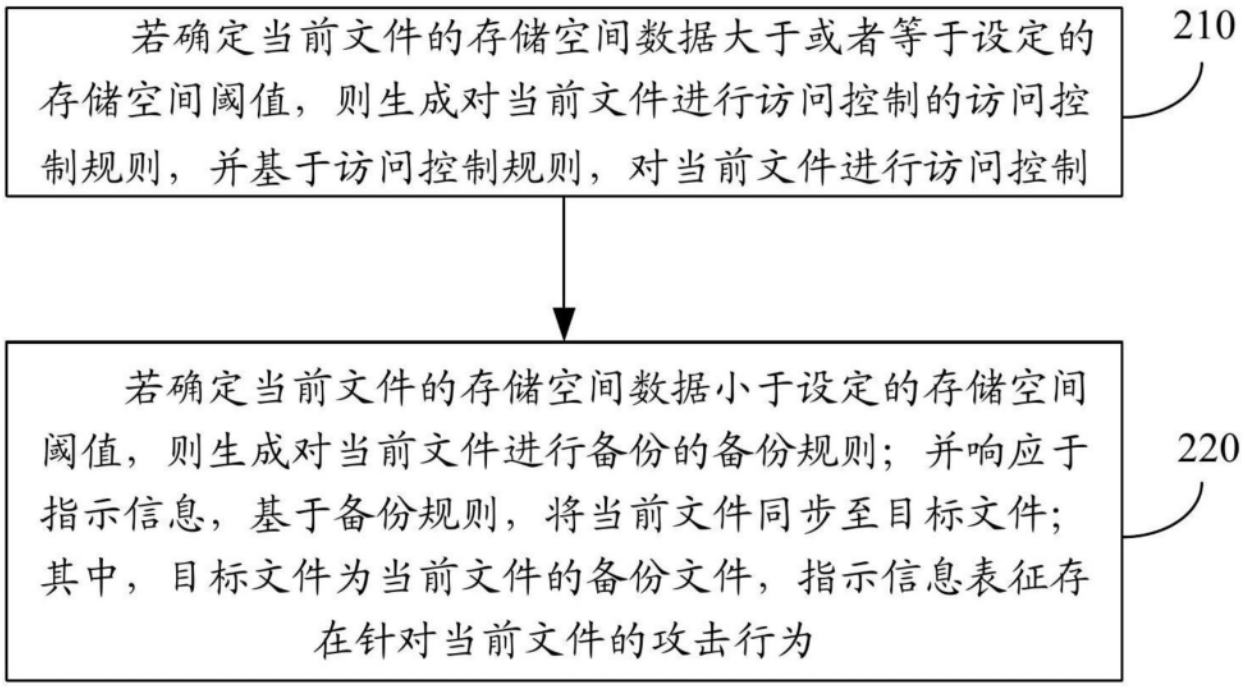
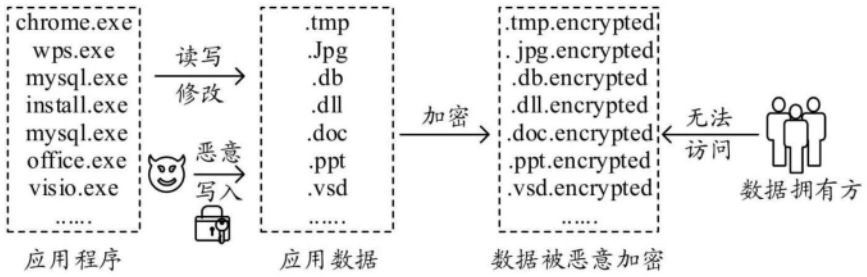

若确定当前文件的存储空间数据大于或者等于设定的存储空间阈值，则生成对当前文件进行访问控制的访问控制规则，并基于访问控制规则，对当前文件进行访问控制
210
若确定当前文件的存储空间数据小于设定的存储空间阈值，则生成对当前文件进行备份的备份规则；并响应于指示信息，基于备份规则，将当前文件同步至目标文件；其中，目标文件为当前文件的备份文件，指示信息表征存在针对当前文件的攻击行为
220

图 2


chrome.exe
wps.exe
mysql.exe
install.exe
mysql.exe
office.exe
visio.exe
.....
读写
修改
恶意
写入
应用程序
.tmp
.Jpg
.db
.dll
.doc
.ppt
.vsd
.....
应用数据
加密
.tmp.encrypted
. jpg.encrypted
.db.encrypted
.dll.encrypted
.doc.encrypted
.ppt.encrypted
.vsd.encrypted
.....
数据被恶意加密
无法
访问
数据拥有方

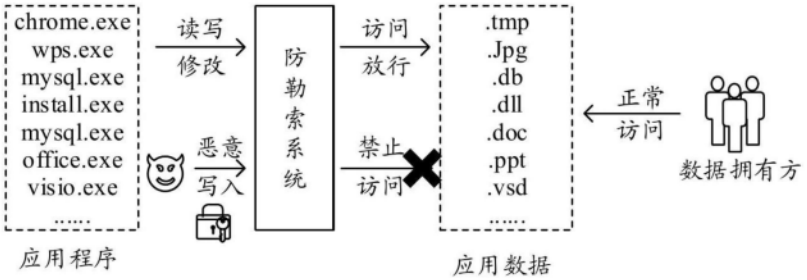

chrome.exe
wps.exe
mysql.exe
install.exe
mysql.exe
office.exe
visio.exe
.....
应用程序
读写
修改
恶意
写入
防勒索系统
访问
放行
禁止
访问
.tmp
.Jpg
.db
.dll
.doc
.ppt
.vsd
.....
应用数据
正常
访问
数据拥有方

图 3

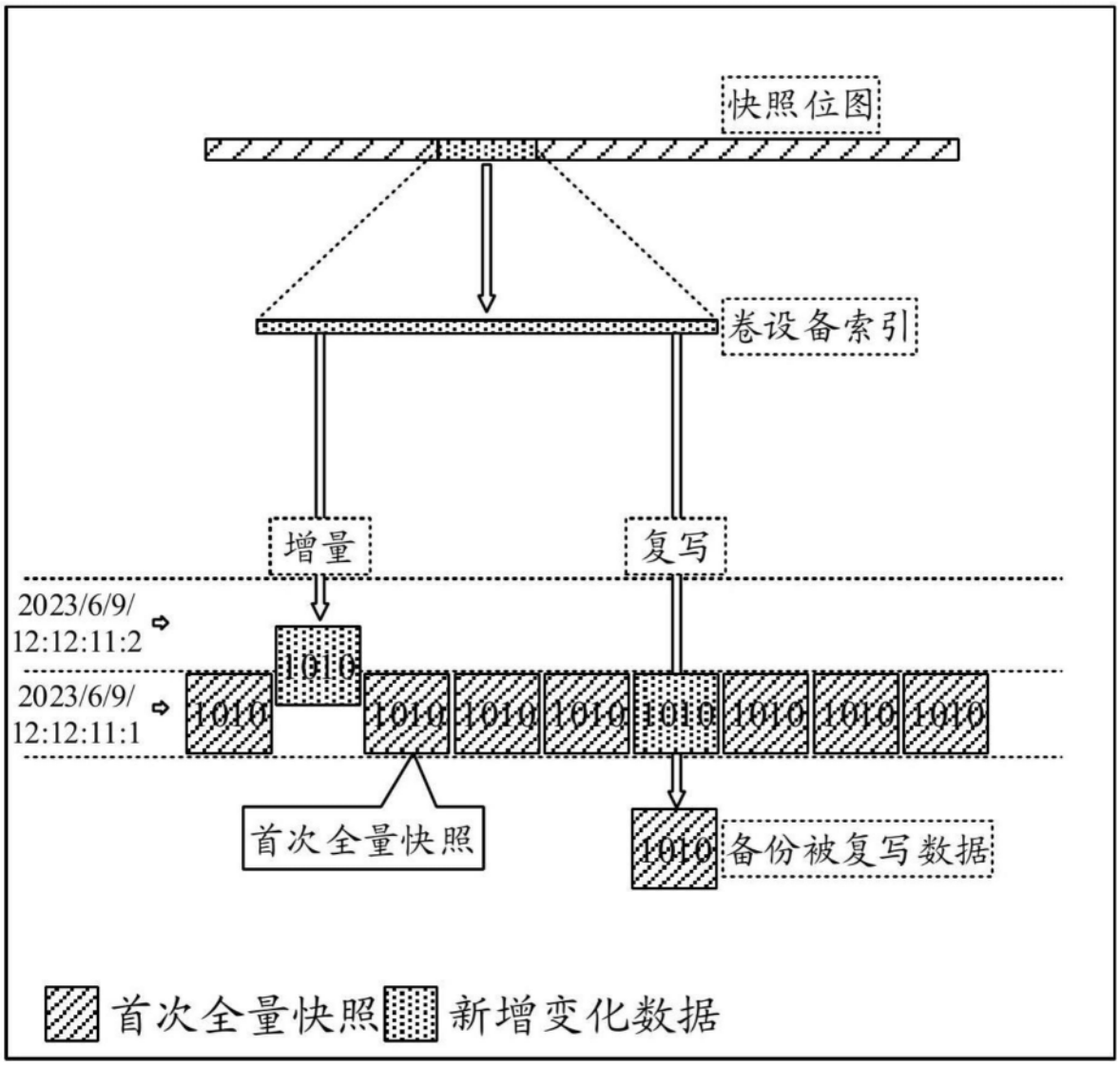

快照位图
卷设备索引
增量
复写
2023/6/9/
12:12:11:2
2023/6/9/
12:12:11:1
1010
首次全量快照
备份被复写数据
首次全量快照
新增变化数据

图 4

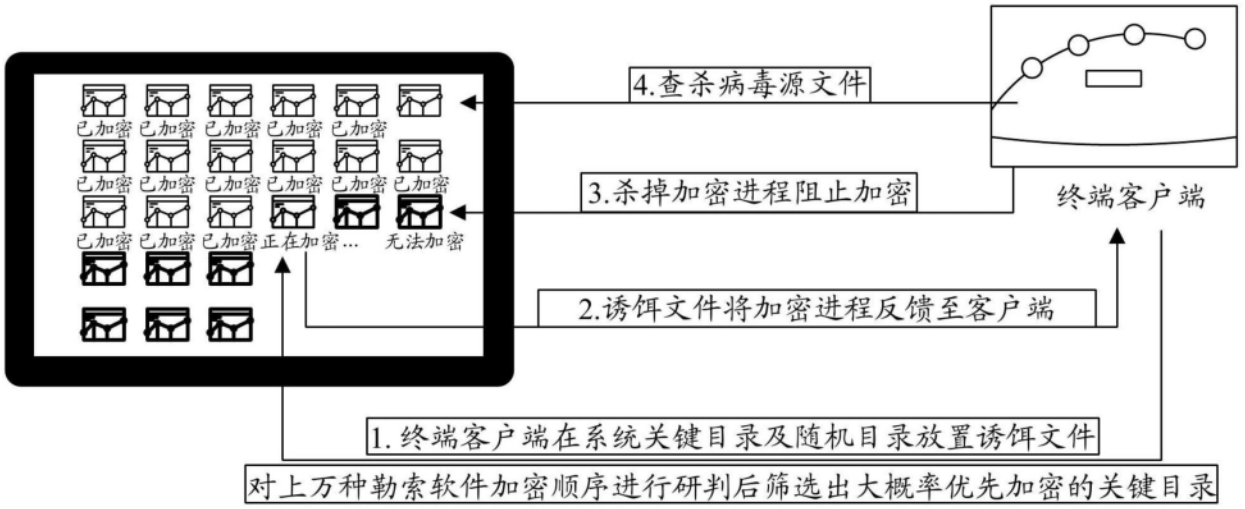

4.查杀病毒源文件
3.杀掉加密进程阻止加密
终端客户端
2.诱饵文件将加密进程反馈至客户端
1.终端客户端在系统关键目录及随机目录放置诱饵文件
对上万种勒索软件加密顺序进行研判后筛选出大概率优先加密的关键目录
已加密
正在加密...
无法加密

图 5

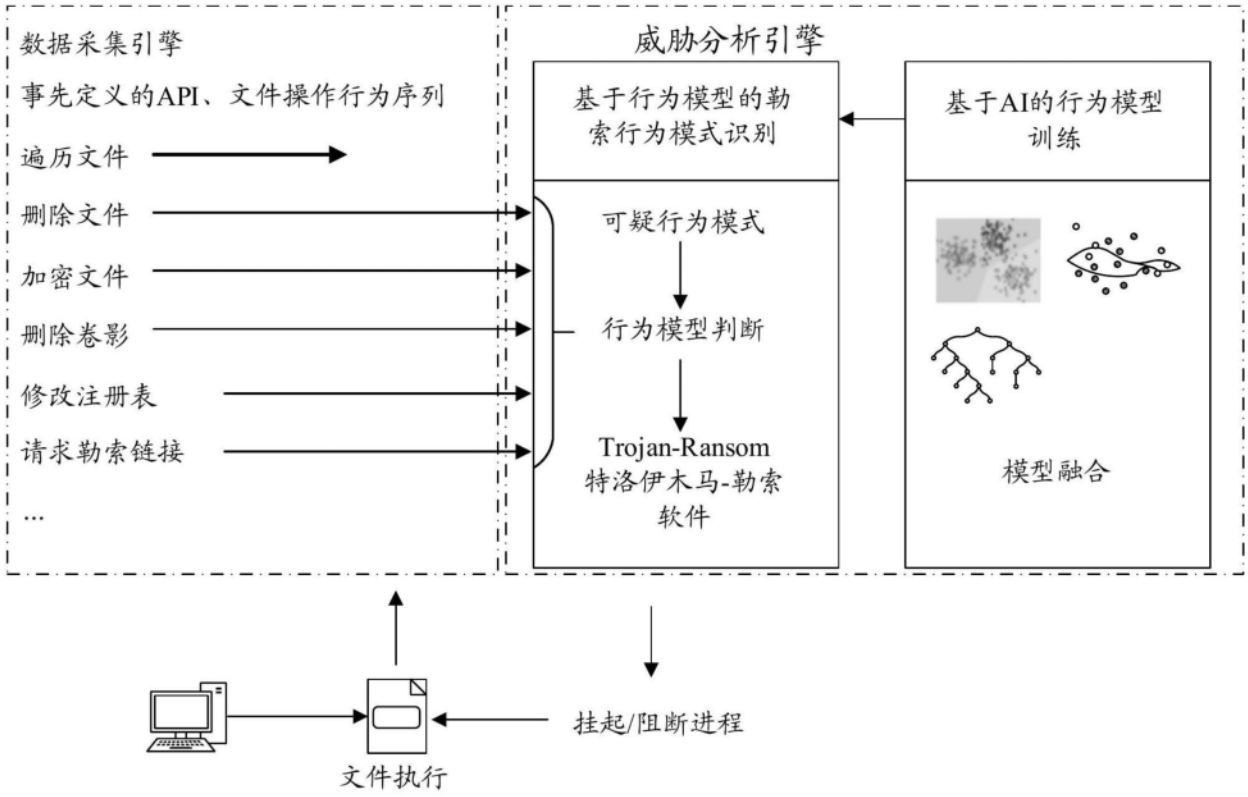

数据采集引擎
事先定义的API、文件操作行为序列
遍历文件
删除文件
加密文件
删除卷影
修改注册表
请求勒索链接
...
威胁分析引擎
基于行为模型的勒索行为模式识别
基于AI的行为模型训练
可疑行为模式
行为模型判断
Trojan-Ransom
特洛伊木马-勒索软件
模型融合
挂起/阻断进程
文件执行

图 6

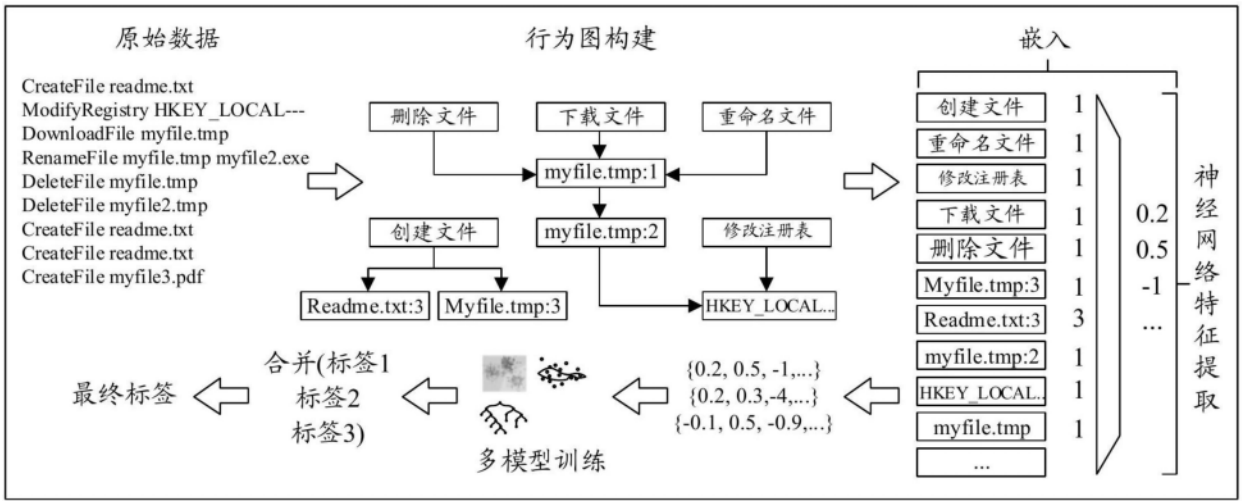

原始数据
行为图构建
嵌入
CreateFile readme.txt
ModifyRegistry HKEY_LOCAL---
DownloadFile myfile.tmp
RenameFile myfile.tmp myfile2.exe
DeleteFile myfile.tmp
DeleteFile myfile2.tmp
CreateFile readme.txt
CreateFile readme.txt
CreateFile myfile3.pdf
删除文件
下载文件
重命名文件
myfile.tmp:1
创建文件
myfile.tmp:2
修改注册表
Readme.txt:3
Myfile.tmp:3
HKEY_LOCAL...
创建文件 1
重命名文件 1
修改注册表 1
下载文件 1
删除文件 1
Myfile.tmp:3 1
Readme.txt:3 3
myfile.tmp:2 1
HKEY_LOCAL... 1
myfile.tmp 1
...
0.2
0.5
-1
...
神经网络特征提取
{0.2, 0.5, -1,...}
{0.2, 0.3,-4,...}
{-0.1, 0.5, -0.9,...}
多模型训练
合并(标签1
标签2
标签3)
最终标签

图 7


技术方案
试点应用展示
重点行业
钢铁行业
化工行业
汽车行业
展示方案
安全态势感知
勒索攻击防护
攻击溯源处置
威胁监测发现
勒索威胁狩猎
高自动化智能运维
子任务5：工业互联网企业勒索智能识别多场景应用验证
核心能力模块
子任务4：勒索软件破解子系统
勒索攻击漏洞协议破解技术资源池
主流加密算法分析模块
勒索软件漏洞分析模块
勒索处置与响应
备份内容一键回滚
全域响应策略下发
轻量备份机制触发
事件定性与故事线构建
勒索加密/窃取进程阻断
可疑远程控制二次验证
风险响应层
动态实时备份
基于访问控制的大文件保护
基于AI的小文件备份
增量快照备份
基于vss的增量快照备份
勒素软件删除卷影防护
子任务3：勒索攻击轻量备份与数据恢复子系统
勒索数据恢复
端侧自动恢复技术
云侧备份恢复技术
恶意行为动态识别系统
基于人工智能的勒索攻击关联分析识别技术
基于信息熵的勒索攻击识别与备份触发技术
基于蜜饵系统的勒索加密/数据窃取动态诱捕技术
基于智能访问控制的关键数据加密保护技术
勒索攻击分析与智能识别层
勒索样本特征分析（二进制反汇编+沙箱动态分析）
勒索攻击行为特征库（通用+专用）
AI模型训练平台
部署优化与迭代测试层
计算框架与算法模型层
数据特征萃取存储层
软硬件架构层
活跃勒索样本收集（加壳、混淆等）
工业互联网环境构建（含主流工业数据库）
动静结合智能防御模块
恶意软件/流量静态分析系统
勒索病毒静态特征匹配模块（AI引擎+规则引擎+文件指纹+证书信息）
文件/流量提取模块（常规脱壳/解混淆+语法语义引擎+虚拟执行引擎）
数据采集模块
攻击事件
文件落地
注册表项
命令执行
进程API
文件追踪
资源占用
网络行为
子任务1：勒索行为特征库与攻击识别模型子系统
子任务2：勒索攻击精准识别与多重勒索防御子系统

图 8

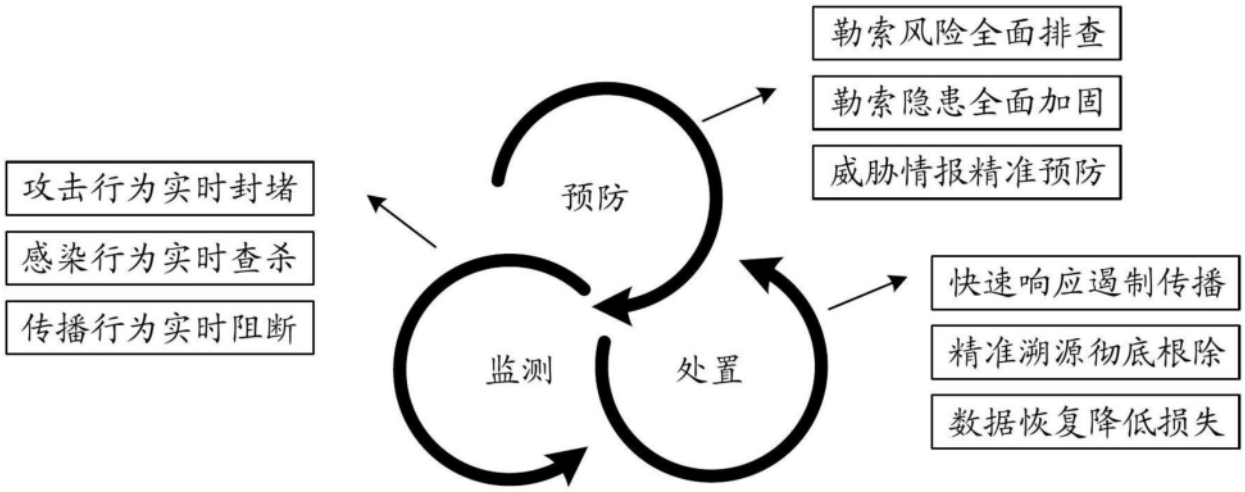

勒索风险全面排查
勒索隐患全面加固
威胁情报精准预防
攻击行为实时封堵
感染行为实时查杀
传播行为实时阻断
预防
监测
处置
快速响应遏制传播
精准溯源彻底根除
数据恢复降低损失

图 9

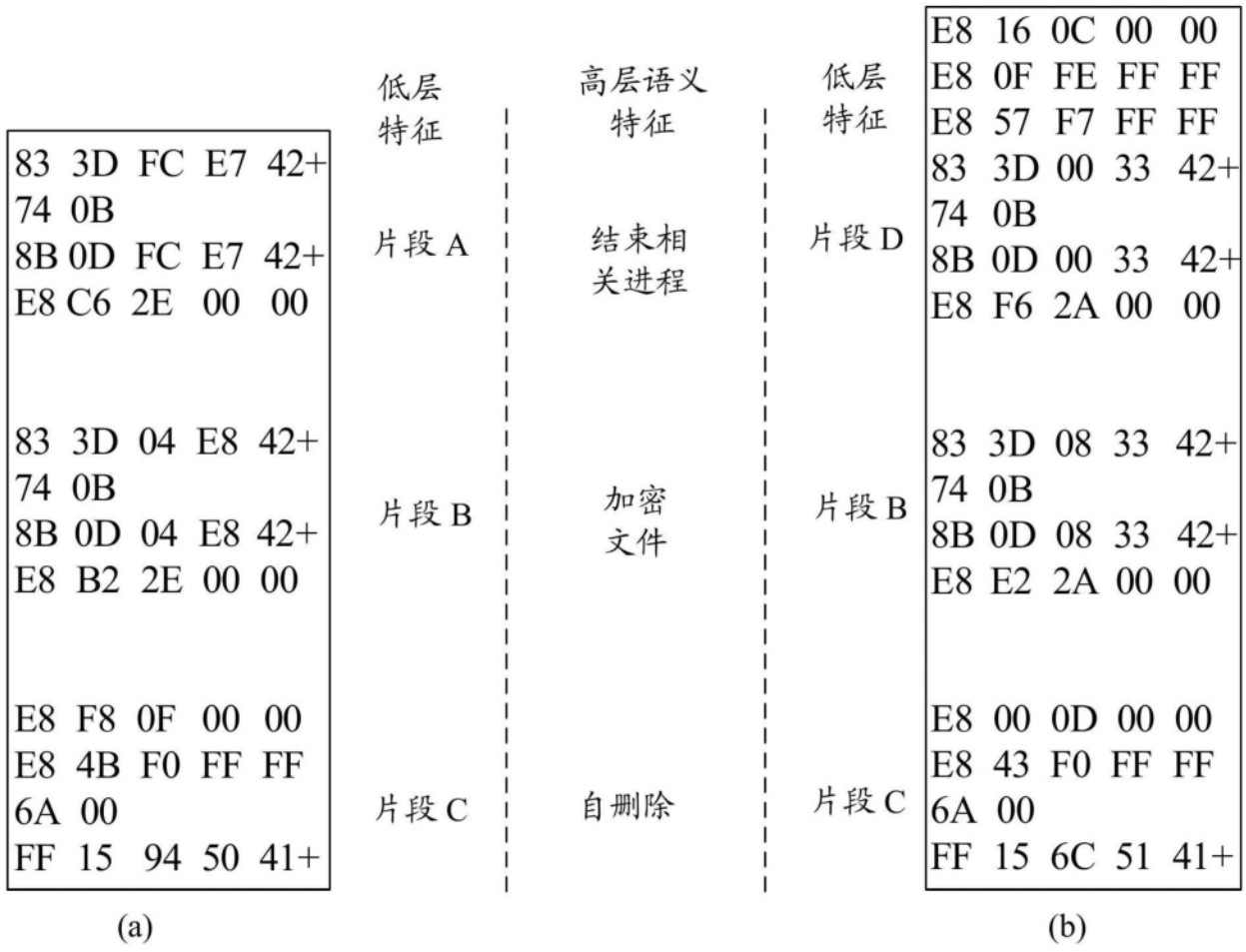

低层特征
高层语义特征
低层特征
83 3D FC E7 42+
74 0B
8B 0D FC E7 42+
E8 C6 2E 00 00
片段 A
结束相关进程
片段 D
E8 16 0C 00 00
E8 0F FE FF FF
E8 57 F7 FF FF
83 3D 00 33 42+
74 0B
8B 0D 00 33 42+
E8 F6 2A 00 00
83 3D 04 E8 42+
74 0B
8B 0D 04 E8 42+
E8 B2 2E 00 00
片段 B
加密文件
片段 B
83 3D 08 33 42+
74 0B
8B 0D 08 33 42+
E8 E2 2A 00 00
E8 F8 0F 00 00
E8 4B F0 FF FF
6A 00
FF 15 94 50 41+
片段 C
自删除
片段 C
E8 00 0D 00 00
E8 43 F0 FF FF
6A 00
FF 15 6C 51 41+
(a)
(b)

图 10

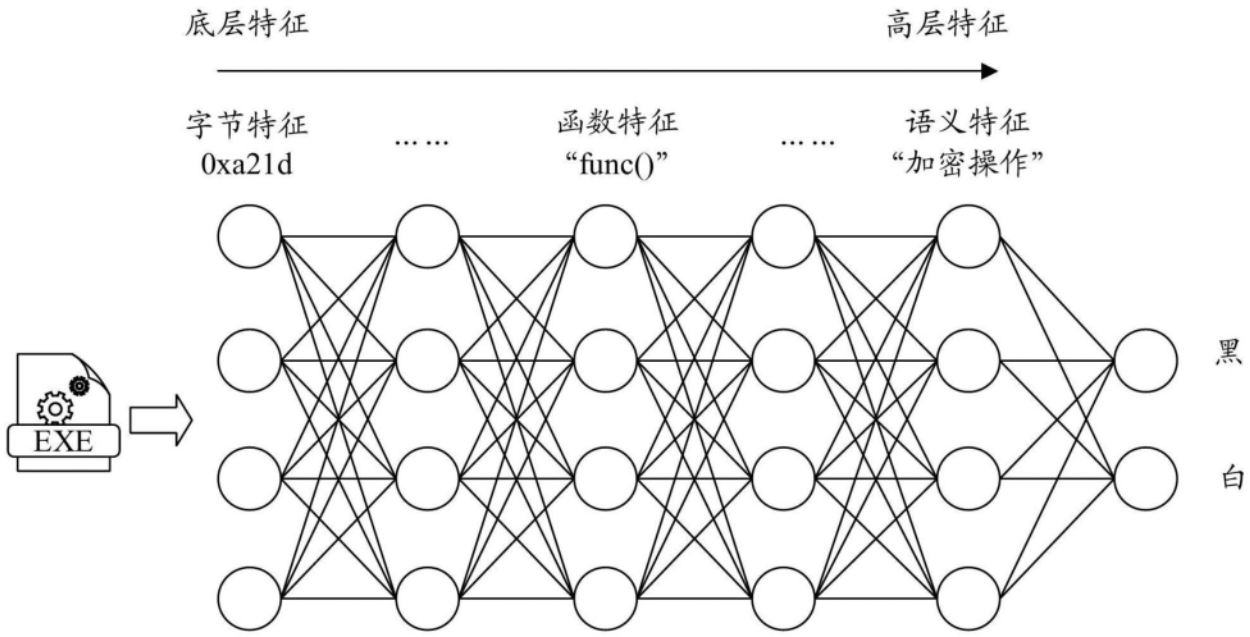

底层特征
高层特征
字节特征
0xa21d
……
函数特征
“func()”
……
语义特征
“加密操作”
EXE
黑
白

图 11

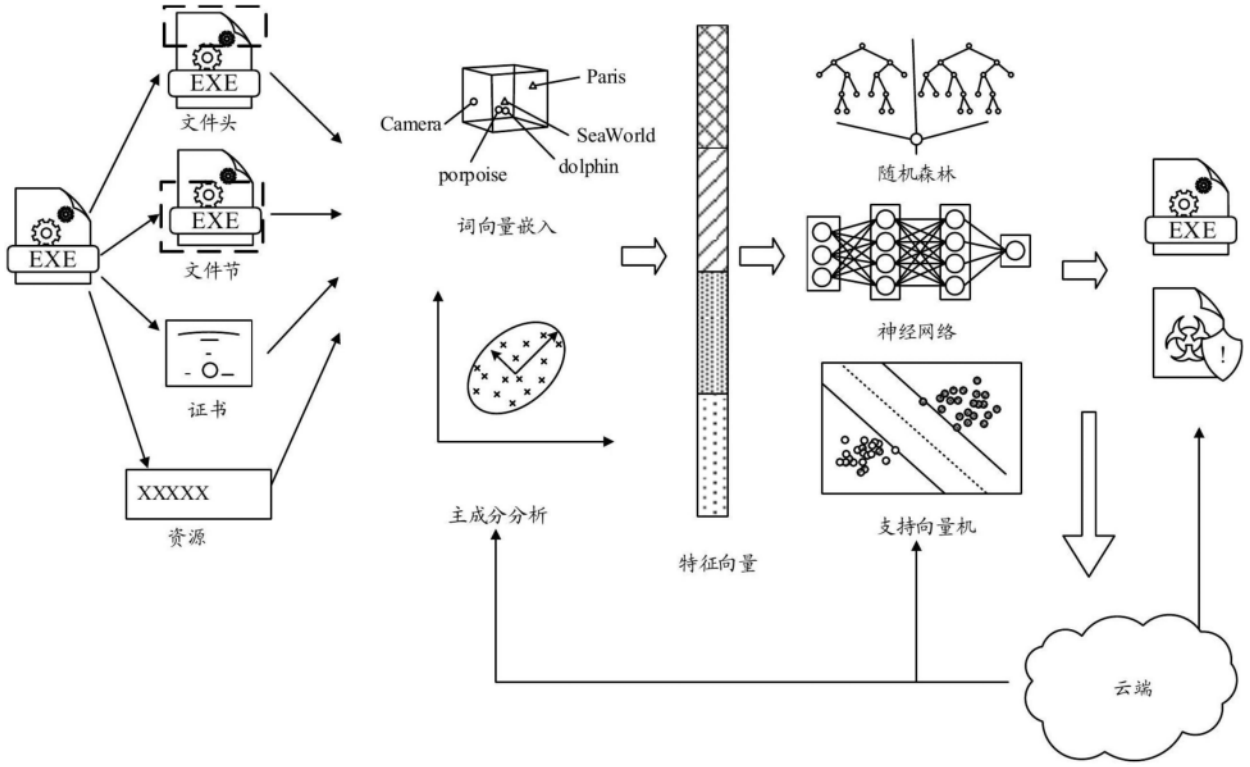

EXE
文件头
EXE
文件节
EXE
证书
XXXXX
资源
Camera
Paris
SeaWorld
porpoise
dolphin
词向量嵌入
主成分分析
特征向量
随机森林
神经网络
支持向量机
EXE
!
云端

图 12

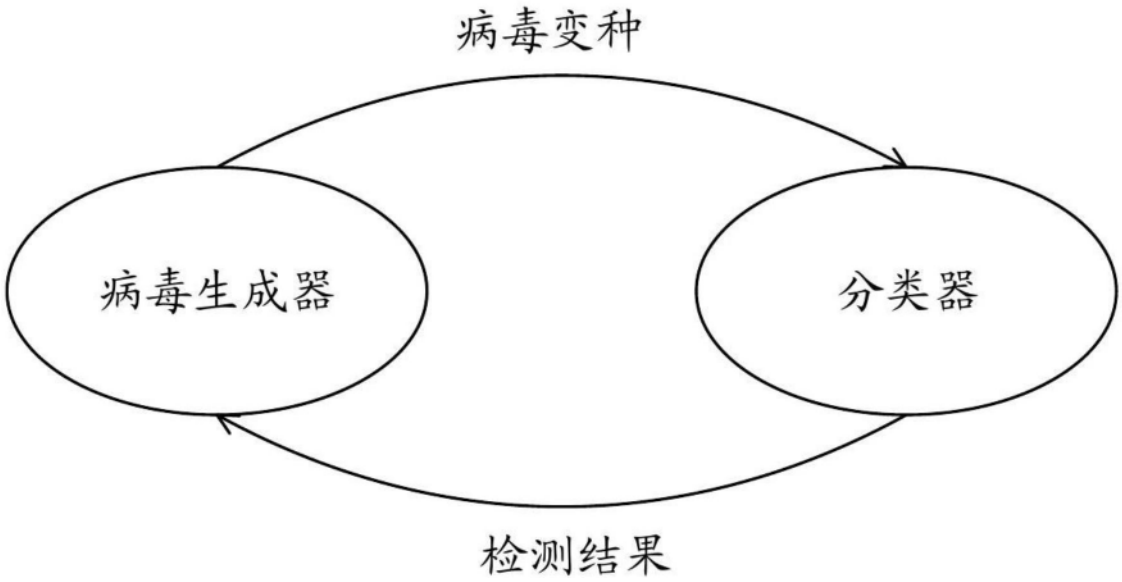

病毒变种
病毒生成器
分类器
检测结果

图 13

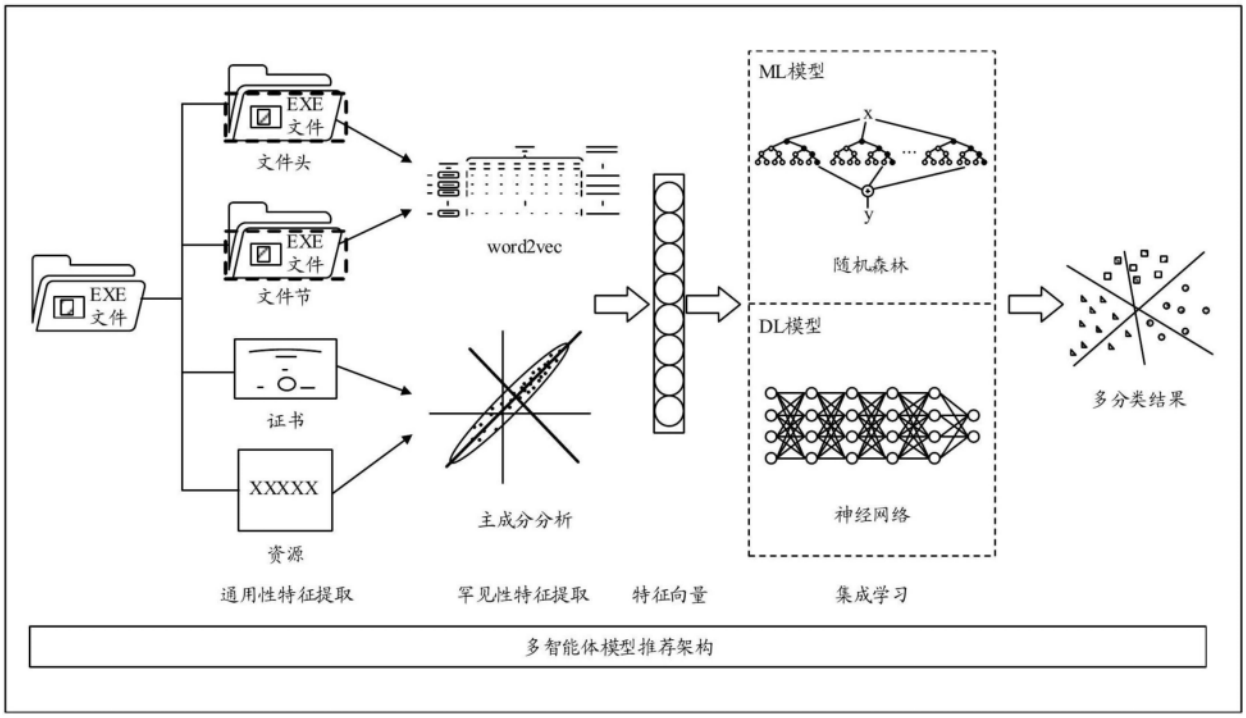

EXE
文件
文件头
EXE
文件
文件节
EXE
文件
证书
XXXXX
资源
word2vec
主成分分析
ML模型
x
y
随机森林
DL模型
神经网络
多分类结果
通用性特征提取
罕见性特征提取
特征向量
集成学习
多智能体模型推荐架构

图 14

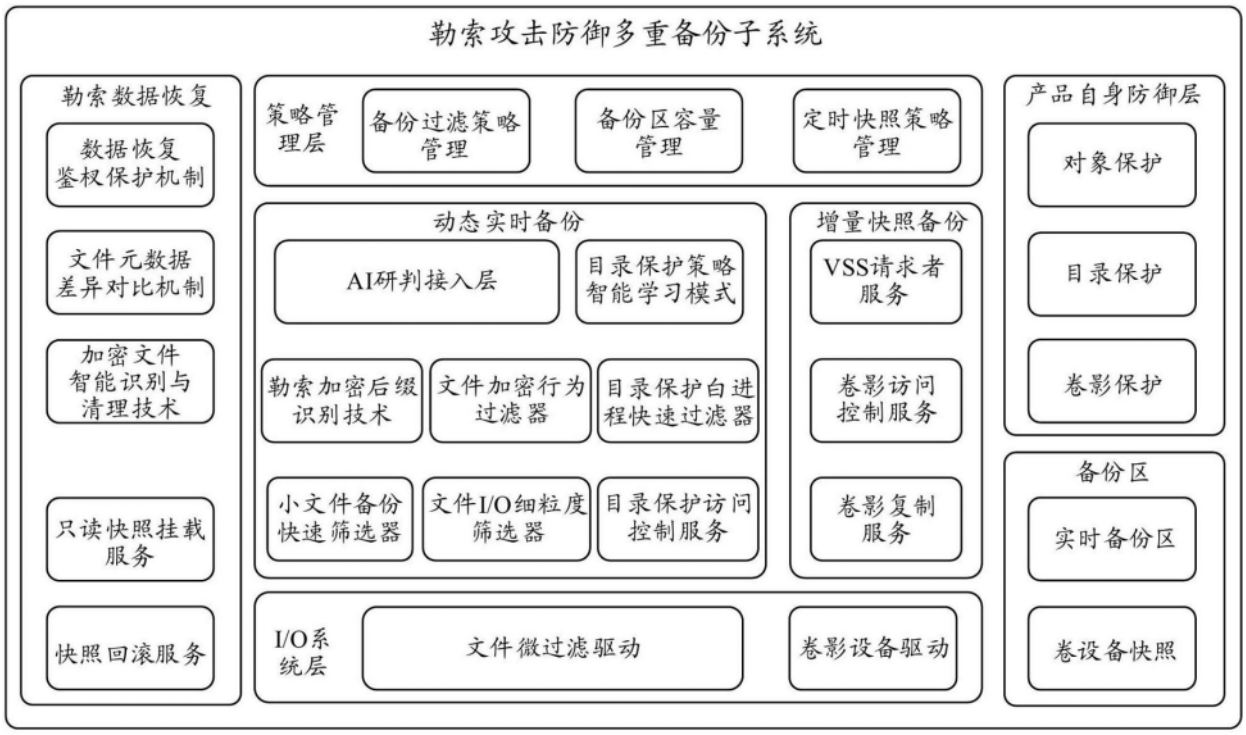

勒索攻击防御多重备份子系统
勒索数据恢复
数据恢复鉴权保护机制
文件元数据差异对比机制
加密文件智能识别与清理技术
只读快照挂载服务
快照回滚服务
策略管理层
备份过滤策略管理
备份区容量管理
定时快照策略管理
动态实时备份
AI研判接入层
目录保护策略智能学习模式
勒索加密后缀识别技术
文件加密行为过滤器
目录保护白进程快速过滤器
小文件备份快速筛选器
文件I/O细粒度筛选器
目录保护访问控制服务
增量快照备份
VSS请求者服务
卷影访问控制服务
卷影复制服务
I/O系统层
文件微过滤驱动
卷影设备驱动
产品自身防御层
对象保护
目录保护
卷影保护
备份区
实时备份区
卷设备快照

图 15

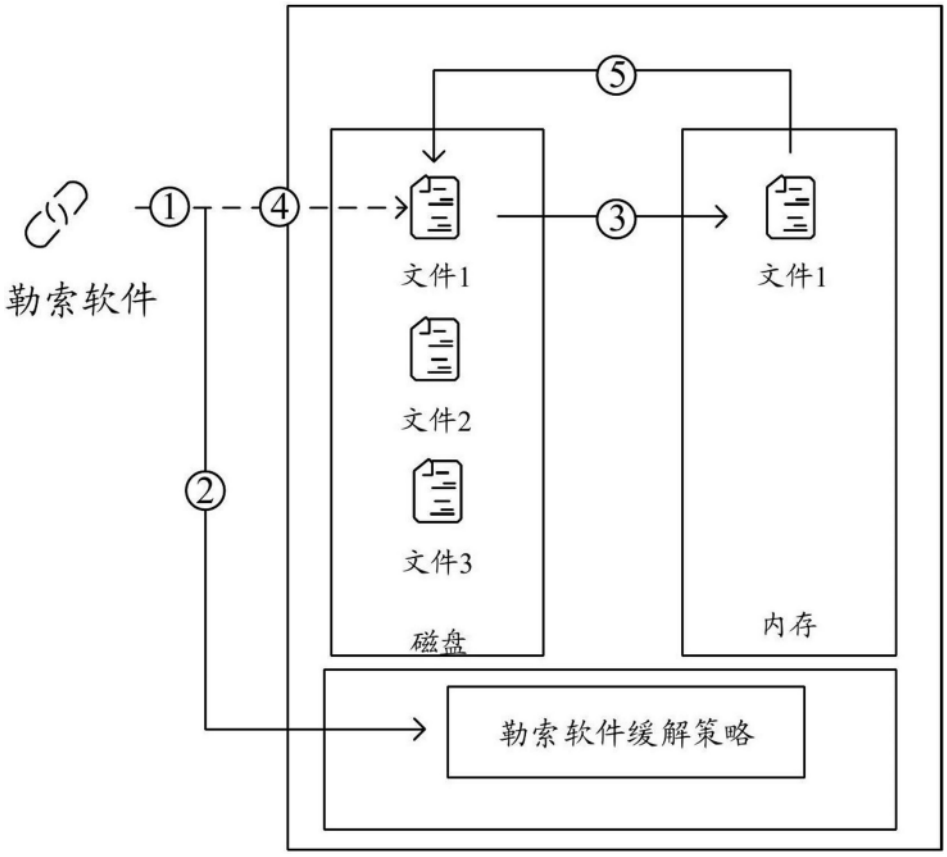

勒索软件
①
②
③
④
⑤
文件1
文件2
文件3
磁盘
文件1
内存
勒索软件缓解策略

图 16

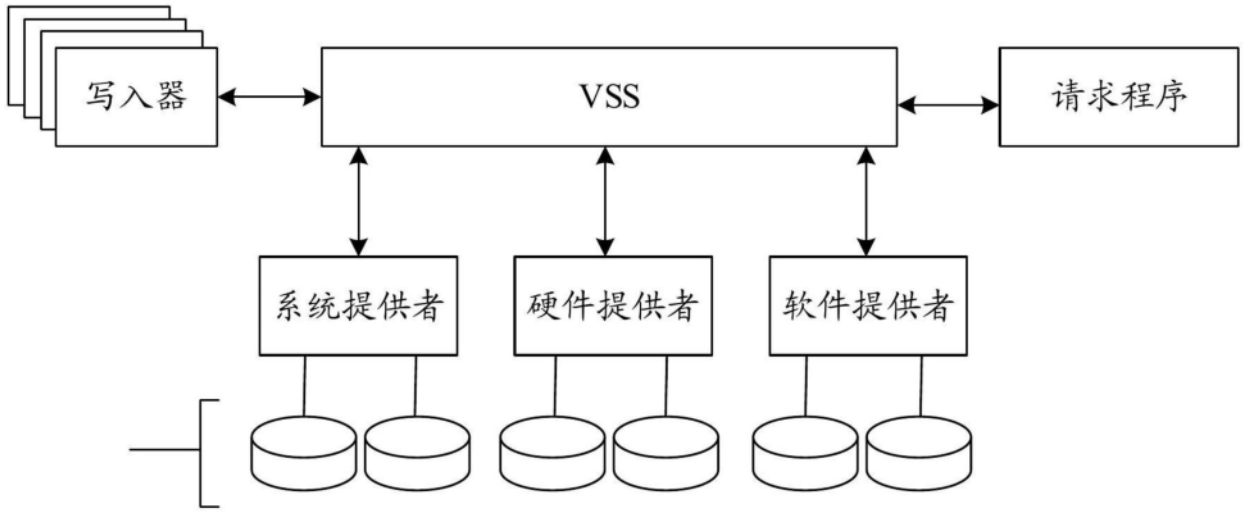

写入器
VSS
请求程序
系统提供者
硬件提供者
软件提供者

图 17

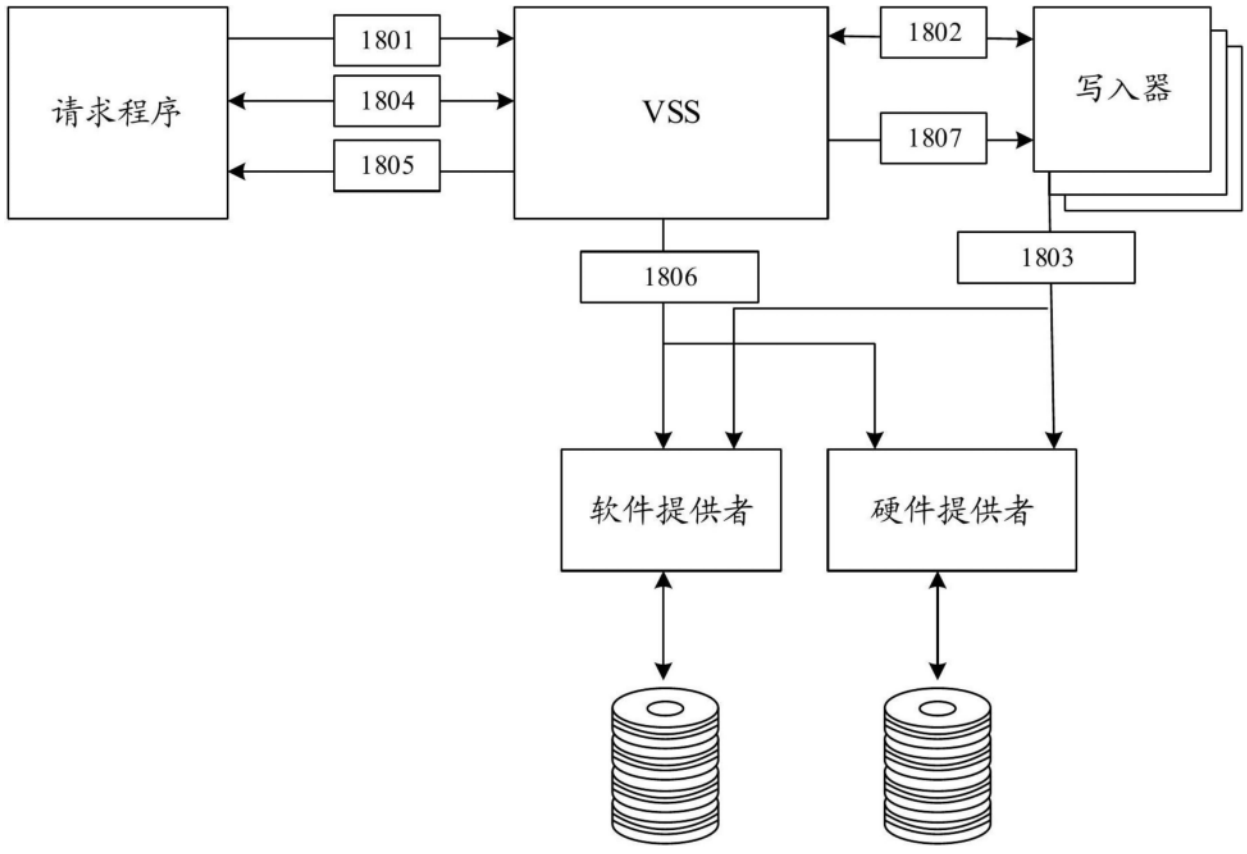

请求程序
1801
1804
1805
VSS
1802
1807
写入器
1806
1803
软件提供者
硬件提供者

图 18

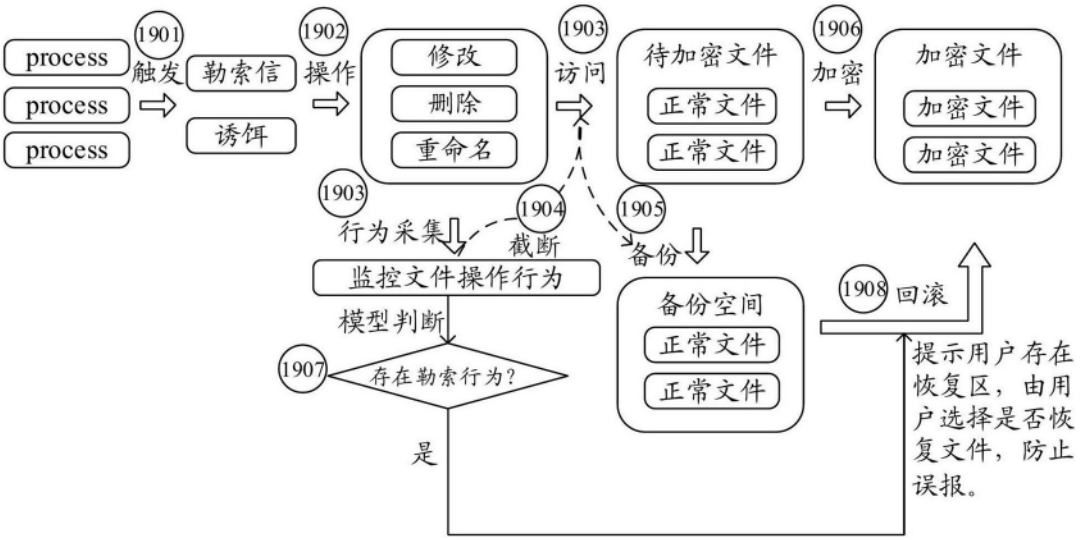

process
process
process
1901
触发
勒索信
诱饵
1902
操作
修改
删除
重命名
1903
访问
待加密文件
正常文件
正常文件
1906
加密
加密文件
加密文件
加密文件
1903
行为采集
1904
截断
1905
备份
监控文件操作行为
模型判断
1907
存在勒索行为?
是
备份空间
正常文件
正常文件
1908
回滚
提示用户存在恢复区，由用户选择是否恢复文件，防止误报。

图 19

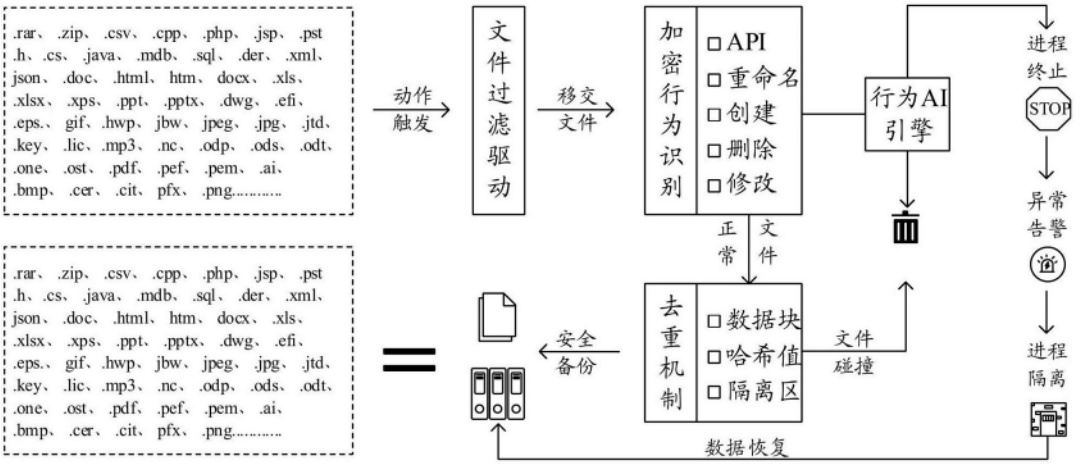

.rar、.zip、.csv、.cpp、.php、.jsp、.pst
.h、.cs、.java、.mdb、.sql、.der、.xml、
json、.doc、.html、htm、docx、.xls、
.xlsx、.xps、.ppt、.pptx、.dwg、.efi、
.eps、gif、.hwp、jbw、jpeg、.jpg、.jtd、
.key、.lic、.mp3、.nc、.odp、.ods、.odt、
.one、.ost、.pdf、.pef、.pem、.ai、
.bmp、.cer、.cit、pfx、.png.....
动作触发
文件过滤驱动
移交文件
加密行为识别
API
重命名
创建
删除
修改
行为AI引擎
进程终止
STOP
异常告警
进程隔离
正常
文件
去重机制
数据块
哈希值
隔离区
文件碰撞
安全备份
数据恢复
.rar、.zip、.csv、.cpp、.php、.jsp、.pst
.h、.cs、.java、.mdb、.sql、.der、.xml、
json、.doc、.html、htm、docx、.xls、
.xlsx、.xps、.ppt、.pptx、.dwg、.efi、
.eps、gif、.hwp、jbw、jpeg、.jpg、.jtd、
.key、.lic、.mp3、.nc、.odp、.ods、.odt、
.one、.ost、.pdf、.pef、.pem、.ai、
.bmp、.cer、.cit、pfx、.png.....

图 20

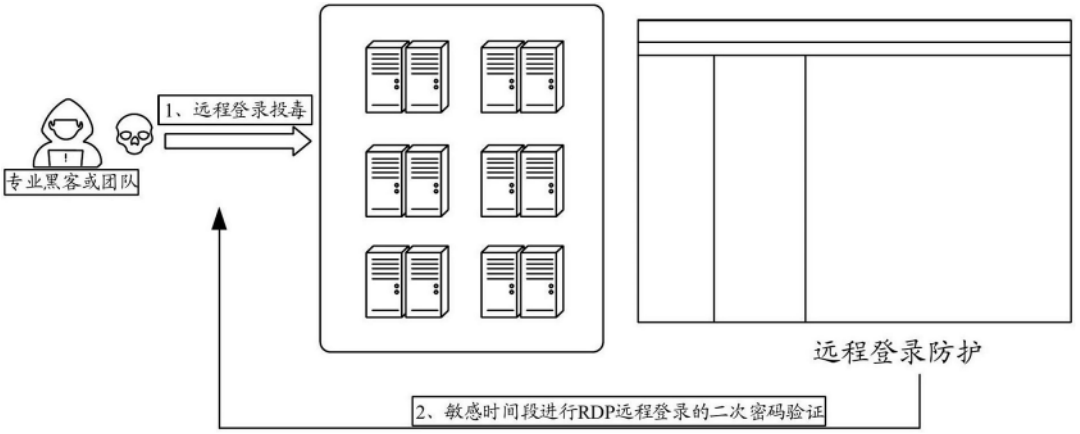

专业黑客或团队
1、远程登录投毒
远程登录防护
2、敏感时间段进行RDP远程登录的二次密码验证

图 21

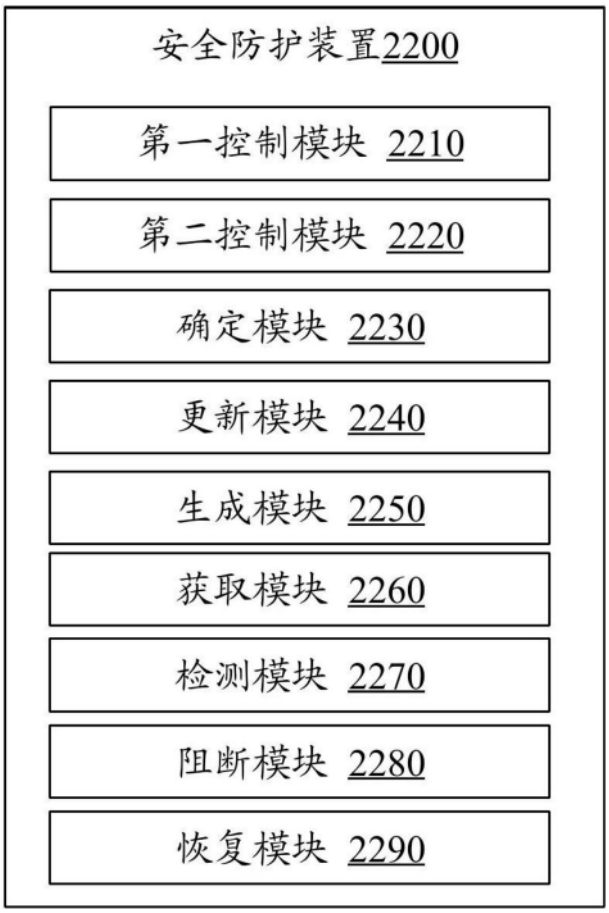

安全防护装置2200
第一控制模块 2210
第二控制模块 2220
确定模块 2230
更新模块 2240
生成模块 2250
获取模块 2260
检测模块 2270
阻断模块 2280
恢复模块 2290

图 22

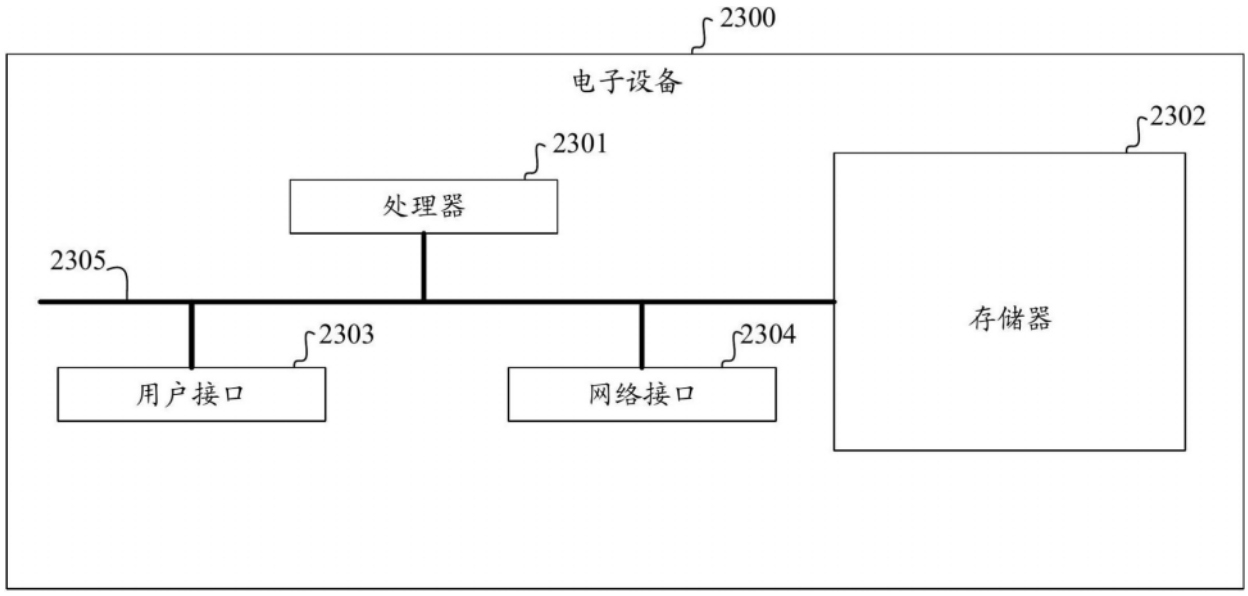

2300
电子设备
2301
处理器
2302
存储器
2305
2303
用户接口
2304
网络接口

图 23