(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102081714 A
(43)申请公布日 2011.06.01

(21)申请号 201110026760.6

(22)申请日 2011.01.25

(71)申请人 潘燕辉
地址 100085 北京市海淀区学清路建清园小区 7 号楼 4 门 701
申请人 周勇兵

(72)发明人 潘燕辉 周勇兵

(51)Int.Cl.
G06F 21/00(2006.01)

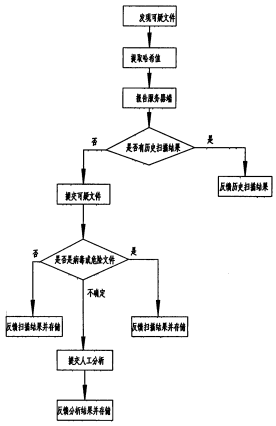
权利要求书 1 页 说明书 3 页 附图 1 页

(54)发明名称

一种基于服务器反馈的云查杀方法

(57)摘要

本发明公开了一种基于服务器反馈的云查杀方法，首先判断所述可疑文件是否由其他用户已经提交并在服务器端进行过扫描，若为否，则将该文件上传至服务器端，在服务器端调用各种杀毒软件进行扫描，将扫描结果反馈给客户端，同时将该扫描结果存储在服务器端的历史扫描结果库中，客户端根据所述扫描结果做出进一步处理；若为是，则所述服务器端直接将存贮在所述历史扫描结果库中的该文件对应的历史扫描结果反馈给所述客户端。同时检查服务器端的杀毒软件及其病毒库，如果杀毒软件病毒库已经更新，或者有新的杀毒软件加入，提示用户是否进行重新扫描，如果用户同意重新扫描，则调用新的杀毒软件和新的病毒库来扫描。



CN 102081714 A

1. 一种基于服务器反馈的云查杀方法，其特征在于，包括至少一客户端和至少一服务器端，所述客户端发现可疑文件以后，将该可疑文件报告给所述服务器端，所述服务器端预安装有多种杀毒软件，首先判断所述可疑文件是否由其他用户已经提交并在服务器端进行过扫描，若为否，则将该文件上传至服务器端，在服务器端调用各种杀毒软件进行扫描，将扫描结果反馈给客户端，同时将该扫描结果存储在服务器端的历史扫描结果库中，客户端根据所述扫描结果做出进一步处理；若为是，则所述服务器端直接将存贮在所述历史扫描结果库中的该文件对应的历史扫描结果反馈给所述客户端，同时检查服务器端的杀毒软件及其病毒库，如果杀毒软件病毒库已经更新，或者有新的杀毒软件加入，提示用户是否进行重新扫描，如果用户同意重新扫描，则调用新的杀毒软件和新的病毒库来扫描。

2. 根据权利要求 1 所述的云查杀方法，其特征在于，所述客户端为计算机、智能手机、掌上电脑之一。

3. 根据权利要求 1 所述的云查杀方法，其特征在于，所述报告可疑文件的方法为：提取可疑文件的哈希值，将所述哈希值上传至所述服务器端。

4. 根据权利要求 1 所述的云查杀方法，其特征在于，所述可疑文件的范围限定在系统中正在运行的可执行文件、驱动及服务、以及调用的各种 DLL 文件中。

一种基于服务器反馈的云查杀方法

技术领域

[0001] 本发明涉及计算机安全技术领域，尤其涉及一种基于服务器反馈的云查杀方法。

背景技术

[0002] 现今，随着信息化程度的提高及各种适用性技术的不断推出，用户进行各种与数字信息相关的活动也越发便利，而且不可否认的是，用户与信息化、数字化的关联也越发紧密。然而与此相随，数字信息犯罪诸如攻击（尤其是通过互联网）个人电脑、服务器、或者其他计算机化装置的事件却频繁发生。显然的是，目前地下数字经济已日益产业化、规模化，而且其相应的犯罪行为也越趋隐蔽化，恶意软件的攻击手段得到了极大的发展。诸如由以前的单个文件发展为多模块、多组件化的攻击的形式，更甚至多数恶意软件均具有较强的伪装能力。

[0003] 目前在多数客户端计算机中，多数只安装一种杀毒软件，最多安装三种杀毒软件，但是问题在于，没有任何一种杀毒软件可以扫描所有的病毒。同时，如果建议客户安装各种杀毒软件也不现实，因为杀毒软件体积巨大，互相之间还可能会有冲突，导致单个客户端很难同时安装多种杀毒软件。这就带来了新的需要解决的技术问题。本发明由此产生。

发明内容

[0004] 本发明所要解决的技术问题是针对现有技术的不足提供一种可以集成多种杀毒软件功能的基于服务器端向客户端反馈的云查杀方法。

[0005] 本发明采用如下技术方案：

[0006] 一种基于服务器反馈的云查杀方法，包括至少一客户端和至少一服务器端，所述客户端发现可疑文件以后，将该可疑文件报告给所述服务器端，所述服务器端预安装有多种杀毒软件，首先判断所述可疑文件是否由其他用户已经提交并在服务器端进行过扫描，若为否，则将该文件上传至服务器端，在服务器端调用各种杀毒软件进行扫描，将扫描结果反馈给客户端，同时将该扫描结果存储在服务器端的历史扫描结果库中，客户端根据所述扫描结果做出进一步处理；若为是，则所述服务器端直接将存贮在所述历史扫描结果库中的该文件对应的历史扫描结果反馈给所述客户端，同时检查服务器端的杀毒软件及其病毒库，如果杀毒软件病毒库已经更新，或者有新的杀毒软件加入，提示用户是否进行重新扫描，如果用户同意重新扫描，则调用新的杀毒软件和新的病毒库来扫描。

[0007] 所述客户端为计算机、智能手机、掌上电脑之一。

[0008] 进一步的，所述报告可疑文件的方法为：提取可疑文件的哈希 (hash) 值，将所述哈希值上传至所述服务器端。

[0009] 优选的，其中所述可疑文件的范围限定在系统中正在运行的可执行文件、驱动及服务、以及调用的各种 DLL 文件中。将上报的文件总量大大的减少，从而实现先对比文件的 HASH 值，然后将没有扫描过的文件上传至服务器进行扫描，大大提高了效率。

[0010] 病毒没有被执行的时候，并不具备危险性，因此只针对正在运行的文件进行扫描，

可以确保目前系统的安全。

附图说明

[0011] 图 1 为本发明系统结构示意图；

[0012] 图 2 为本发明方法流程图。

具体实施方式

[0013] 以下结合具体实施例，对本发明进行详细说明。

[0014] 如图 1、2 所示，一种基于服务器反馈的云查杀方法，用于客户端与服务器端通过互联网对本地用户系统（例如计算机、掌上电脑、智能手机等用户终端）进行病毒的查杀，当用户终端发现可疑文件以后，要求对该可疑文件进行查毒操作时，所述客户端程序模块 11 从所述客户终端 1 的本地文件系统中获取该可疑文件 121 的 hash 值，可以采用常用 hash 算法有：sha、sha1、sha256 以及 md5 等。其他还有 md4、md2、mdc2 以及 ripemd160 等。

[0015] 可疑文件的范围限定在系统中正在运行的可执行文件、驱动及服务、以及调用的各种 DLL 文件中。将上报的文件总量大大的减少，从而实现先对比文件 HASH，然后将没有扫描过的文件上传至服务器进行扫描，大大提高了效率。

[0016] 所述客户端程序模块 11 将该 hash 值报告给所述服务端程序模块 21，试图在服务器端查询该可疑文件 121 的文件是否为病毒或危险文件；

[0017] 所述服务端程序模块 21 在所述服务器端 2 的历史扫描结果数据库 22 中检索该 hash 值，如果发现该 hash 值已经存在，即表明曾经有用户提交过该文件的扫描请求，在历史扫描结果数据库 22 中存储有该可疑文件的扫描结果，则所述服务器端程序模块 21 向所述客户端程序模块 11 返回该 hash 值对应的历史扫描结果；同时，检查服务器端的杀毒软件及其病毒库，如果杀毒软件病毒库已经更新，或者有新的杀毒软件加入，提示用户是否进行重新扫描，如果用户同意重新扫描，则调用新的杀毒软件和新的病毒库来扫描。

[0018] 如果该 hash 值不存在，则所述服务器端程序模块 21 要求所述客户端程序模块 11 将该可疑文件 121 上传到所述服务器端 2，并且使用安装在所述服务器端 2 的杀毒引擎 22 或者杀毒引擎 23 或者 24 等一系列杀毒引擎进行查毒操作；

[0019] 如果在该待查毒文件中发现病毒，则所述服务器端程序模块 21 将查毒结果返回给所述客户端程序模块 11，并且向所述服务器端 2 的历史扫描结果数据库添加该查毒文件 121 对应的 hash 值、文件类型以及病毒名；

[0020] 如果在该待查毒文件 121 中没有发现病毒或者危险文件，则所述服务器端程序模块 21 将该可疑文件记为“未发现病毒”，将此结果返回给所述客户端程序模块 11。同时，将该待查毒文件提交给病毒分析员作人工处理；当人工分析完成后，如果是正常文件，将获取的该文件的校验值、文件类型及其他信息更新到所述服务器端 2 的历史扫描结果数据库中；经过人工分析以后，发现病毒，病毒分析员将提取该病毒的特征码并且更新至所述服务器端 2 的杀毒引擎病毒库，并将该结果反馈给客户端。

[0021] 这样在客户端可以不安装杀毒引擎即可实现对可疑文件的杀毒扫描操作，大大节约客户端的系统资源，另外通过对历史扫描结果数据库的检索，可以大大节约向用户反馈的时间。

[0022] 应当理解的是，对本领域普通技术人员来说，可以根据上述说明加以改进或变换，而所有这些改进和变换都应属于本发明所附权利要求的保护范围。

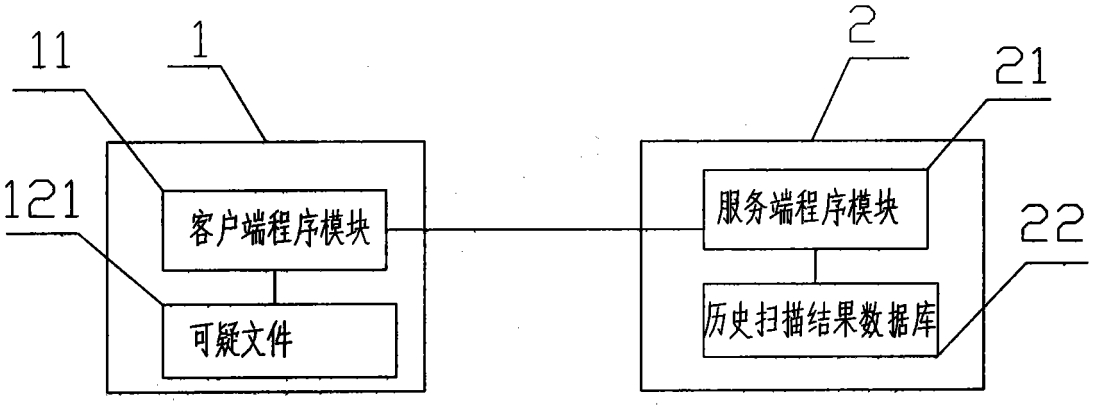

11
1
2
21
121
客户端程序模块
服务端程序模块
22
可疑文件
历史扫描结果数据库

图 1

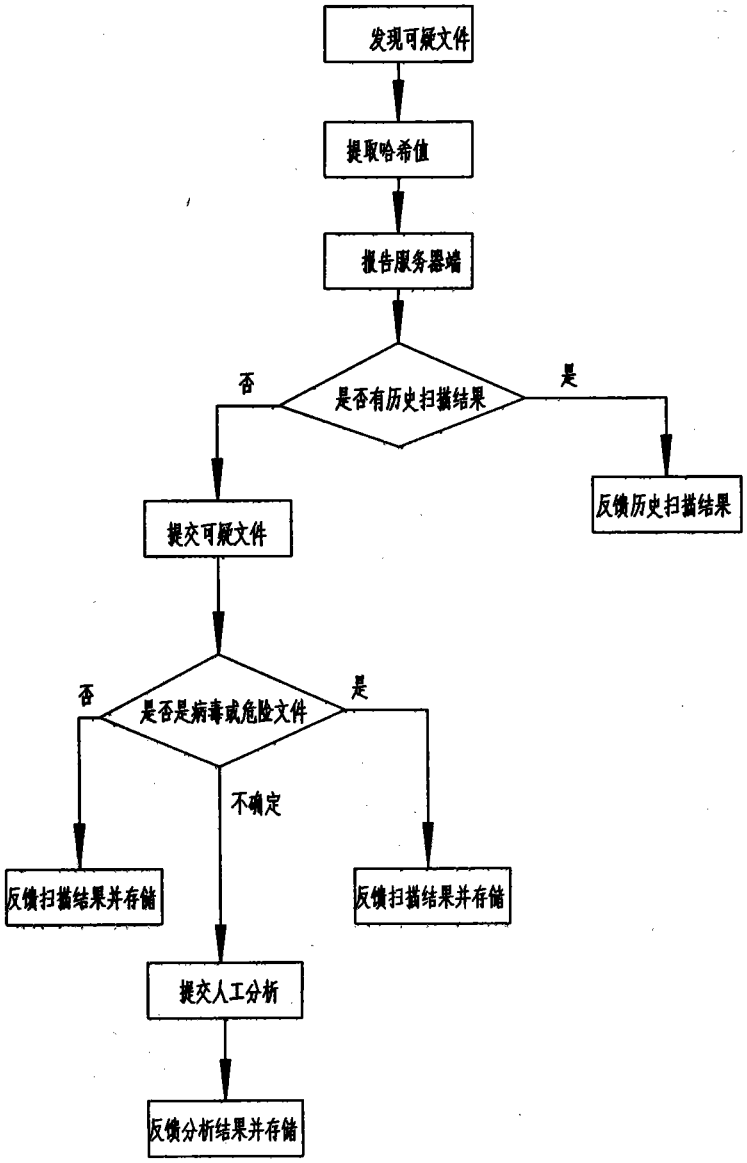

发现可疑文件
提取哈希值
报告服务器端
是否有历史扫描结果
否
是
反馈历史扫描结果
提交可疑文件
是否是病毒或危险文件
否
是
不确定
反馈扫描结果并存储
反馈扫描结果并存储
提交人工分析
反馈分析结果并存储

图 2