(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 102855420 B
(45)授权公告日 2015.08.19

(21)申请号 201210302231.9

(22)申请日 2012.08.23

(73)专利权人 珠海市君天电子科技有限公司
地址 519000 广东省珠海市唐家湾镇港湾大道科技一路 10 号主楼 6 层 601F

(72)发明人 黄舰 梁宇杰 赵昱 陈勇

(74)专利代理机构 北京柏杉松知识产权代理事务所（普通合伙） 11413
代理人 马敬

(51)Int.Cl.
G06F 21/10(2013.01)

(56)对比文件
CN 102346828 A,2012.02.08, 说明书第【0002】段 -【0081】段 .
CN 102081714 A,2011.06.01, 全文 .
GODDOFER. “KSC 云启发引擎”. 《HTTP://BAIKE.BAIDU.COM/HISTORY/27613394》. 2012,

审查员 金梦

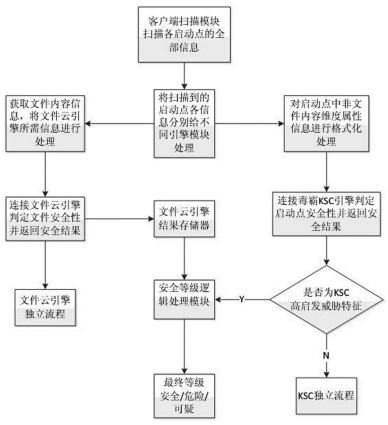
权利要求书2页 说明书3页 附图1页

(54)发明名称

一种多维度引擎间联合判定启动点安全性的启发检测方法

(57)摘要

本发明公开了一种多维度引擎间联合判定启动点安全性的启发检测方法，包括以下步骤：a. 客户端扫描启动点；b. 将启动点信息提交给文件云引擎进行文件内容信息获取，以及将启动点信息提交给毒霸 KSC 引擎；c. 文件云引擎对文件内容的安全性进行判断并返回安全结果，毒霸 KSC 引擎对启动点的安全性进行判断并返回安全结果；d. 根据返回安全结果判断是否提交给安全等级逻辑处理模块；e. 确定最终安全等级。所述方法把不同引擎联合起来，在一个启动点中取各引擎最优势的信息，综合分析后来判定启动点的安全性等级，最终实现启动点的安全性判定，更可靠、更安全。本发明多维度引擎间联合判定启动点安全性的启发检测方法广泛应用于安全检测技术领域。



CN 102855420 B

1. 一种多维度引擎间联合判定启动点安全性的启发检测方法，其特征在于，该方法包括以下步骤：

a. 客户端扫描启动点；

b. 获取各启动点的信息，将扫描到的启动点信息分配给不同的引擎模块进行处理，包括：将扫描到的启动点信息分配给不同的引擎模块进行处理包括将启动点的内容信息提交给文件云引擎进行文件内容信息获取，以及将启动点中非文件内容维度属性信息提交给毒霸 KSC 引擎；

c. 文件云引擎对文件内容的安全性进行判断并返回安全结果，毒霸 KSC 引擎基于高启发威胁特征对启动点的安全性进行判断并返回安全结果；

d. 根据毒霸 KSC 引擎对启动点的安全性进行判断并返回的安全结果，判断是否提交给安全等级逻辑处理模块，其中，当毒霸 KSC 引擎返回的安全结果为高启发威胁状态时，毒霸 KSC 引擎才会把该状态信息传给安全等级逻辑处理模块，毒霸 KSC 引擎还会将启动点的广度信息传给安全等级逻辑处理模块，而文件云引擎的每个状态都会传给安全等级逻辑处理模块；

e. 根据安全等级逻辑处理模块的逻辑确定最终安全等级。

2. 根据权利要求 1 所述的一种多维度引擎间联合判定启动点安全性的启发检测方法，其特征在于，所述步骤 b，其具体为：

将启动点信息提交给文件云引擎进行文件内容信息获取，并对文件云引擎所需信息进行处理，以及将启动点信息提交给毒霸 KSC 引擎，进而对启动点中非文件内容维度属性信息进行格式化处理。

3. 根据权利要求 1 所述的一种多维度引擎间联合判定启动点安全性的启发检测方法，其特征在于，所述步骤 c，其包括：

文件云引擎对文件内容的安全性进行判断，并将返回的安全结果存储起来；毒霸 KSC 引擎对非文件内容维度的启动点安全性进行判断，并判断该安全结果是否为 KSC 高启发威胁特征，若是，则对文件云引擎返回的安全结果进行获取后，将文件云引擎返回的安全结果以及毒霸 KSC 引擎返回的安全结果一起提交给安全等级逻辑处理模块，否则将继续执行 KSC 独立流程。

4. 根据权利要求 2 所述的一种多维度引擎间联合判定启动点安全性的启发检测方法，其特征在于，所述步骤 c 中文件云引擎返回的安全结果存储在文件云引擎结果存储器内。

5. 根据权利要求 2 所述的一种多维度引擎间联合判定启动点安全性的启发检测方法，其特征在于，所述步骤 c 中文件云引擎返回的安全结果包括云 2.0 安全、云 3.0 安全、云 2.0 危险、云 3.0 危险、未知这五种状态，毒霸 KSC 引擎返回的安全结果包括安全、危险、高启发威胁、未知 + 分布广度这四种状态和启动点的广度值。

6. 根据权利要求 4 所述的一种多维度引擎间联合判定启动点安全性的启发检测方法，其特征在于，所述安全等级逻辑处理模块的逻辑为：

如果毒霸 KSC 引擎状态 = 云 3.0 安全，则最终安全等级为安全；

如果毒霸 KSC 引擎状态 = 云 2.0 安全且文件云引擎广度 < 预定阈值，则最终安全等级为可疑；

如果毒霸 KSC 引擎状态 = 云 2.0 安全且文件云引擎广度 >= 预定阈值，则最终安全等级

为安全；

否则，其他情况最终安全等级均为威胁。

一种多维度引擎间联合判定启动点安全性的启发检测方法

技术领域

[0001] 本发明涉及安全检测技术领域，尤其是一种多维度引擎间联合判定启动点安全性的启发检测方法。

背景技术

[0002] 众所周知，基于文件内容维度的检测引擎，已经是安全行业内部最为广泛和成熟的安全检测方式，但近年来随着安全与病毒产业的不断对抗，病毒程序已经逐步告别从前的各种文件内容的修改来躲避文件引擎的扫描，而是逐步转为利用安全的计算机程序的各种漏洞来使病毒文件被运行从而达到危害计算机安全的目的。

[0003] KSC是Kingsoft System Intelligent Cloud的简写，是金山可信云认证体系下的一个系统级别人工智能云体系。毒霸KSC引擎是金山毒霸开发的基于KSC的检测引擎。与基于文件内容维度的检测引擎不同的是，毒霸KSC引擎是基于系统级别云体系的，它无视文件本身信息，转而聚焦文件所处环境——操作系统的多维度安全特征，全面封锁和侦查启动点，在病毒最关键的启动点给予精准致命打击，从而形成了全新的系统安全模式。但是由于KSC高启发规则的高启发特性，会将一部分安全程序但是行为类似病毒的启动点报出造成误报。

[0004] 由此可见，现有安全检测技术大都是基于单一的引擎或者检测方式来进行安全判定的，由于各个引擎及检测方式都存在其固有的优势和缺点，故而使用单一引擎的检测都无法避免其缺点所造成的先天不足。

发明内容

[0005] 本发明要解决的技术问题是：提供一种多维度引擎间联合判定启动点安全性的启发检测方法，克服使用单一引擎检测方式的不足。

[0006] 为了解决上述技术问题，本发明所采用的技术方案是：

[0007] 一种多维度引擎间联合判定启动点安全性的启发检测方法，该方法包括以下步骤：

[0008] a. 客户端扫描启动点；

[0009] b. 将启动点信息提交给文件云引擎进行文件内容信息获取，以及将启动点信息提交给毒霸KSC引擎；

[0010] c. 文件云引擎对文件内容的安全性进行判断并返回安全结果，毒霸KSC引擎对启动点的安全性进行判断并返回安全结果；

[0011] d. 根据返回安全结果判断是否提交给安全等级逻辑处理模块；

[0012] e. 确定最终安全等级。

[0013] 优选地，所述步骤b，其具体为：

[0014] 将启动点信息提交给文件云引擎进行文件内容信息获取，并对文件云引擎所需信息进行处理，以及将启动点信息提交给毒霸KSC引擎，进而对启动点中非文件内容维度属

性信息进行格式化处理。

[0015] 优选地，所述步骤 c，其包括 ：

[0016] 文件云引擎对文件内容的安全性进行判断，并将返回的安全结果存储起来 ；

[0017] 毒霸 KSC 引擎对非文件内容维度的启动点安全性进行判断，并判断该安全结果是否为 KSC 高启发威胁特征，若是，则对文件云引擎返回的安全结果进行获取后，将文件云引擎返回的安全结果以及毒霸 KSC 引擎返回的安全结果一起提交给安全等级逻辑处理模块，否则将继续执行 KSC 独立流程。

[0018] 优选地，所述步骤 c 中文件云引擎返回的安全结果存储在文件云引擎结果存储器内。

[0019] 优选地，所述步骤 c 中文件云引擎返回的安全结果包括云 2.0 安全、云 3.0 安全、云 2.0 危险、云 3.0 危险、未知这五种状态，毒霸 KSC 引擎返回的安全结果包括安全、危险、高启发威胁、未知 + 分布广度这四种状态和启动点的广度值。

[0020] 优选地，所述安全等级逻辑处理模块的逻辑为 ：

[0021] 如果毒霸 KSC 引擎状态 = 云 3.0 安全，则最终安全等级为安全 ；

[0022] 如果毒霸 KSC 引擎状态 = 云 2.0 安全且文件云引擎广度 < 预定阈值，则最终安全等级为可疑 ；

[0023] 如果毒霸 KSC 引擎状态 = 云 2.0 安全且文件云引擎广度 >= 预定阈值，则最终安全等级为安全 ；

[0024] 否则，其他情况最终安全等级均为威胁。

[0025] 本发明的有益效果是 ：本发明不使用单一的引擎来判断启动点的安全性，而是把不同引擎联合起来，在一个启动点中取各引擎最优势的信息，综合分析后来判定启动点的安全性等级，最终实现启动点的安全性判定，更可靠、更安全。

附图说明

[0026] 附图是本发明多维度引擎间联合判定启动点安全性的启发检测方法的步骤流程图。

具体实施方式

[0027] 下面结合附图对本发明的具体实施方式作进一步说明 ：

[0028] 参照附图，一种多维度引擎间联合判定启动点安全性的启发检测方法，该方法包括以下步骤 ：

[0029] a. 客户端扫描启动点 ；

[0030] b. 将启动点信息提交给文件云引擎进行文件内容信息获取，以及将启动点信息提交给毒霸 KSC 引擎 ；

[0031] c. 文件云引擎对文件内容的安全性进行判断并返回安全结果，毒霸 KSC 引擎对启动点的安全性进行判断并返回安全结果 ；

[0032] d. 根据返回安全结果判断是否提交给安全等级逻辑处理模块 ；

[0033] e. 确定最终安全等级。

[0034] 作为进一步优选的实施方式，所述步骤 b，其具体为 ：

[0035] 将启动点信息提交给文件云引擎进行文件内容信息获取，并对文件云引擎所需信息进行处理，以及将启动点信息提交给毒霸 KSC 引擎，进而对启动点中非文件内容维度属性信息进行格式化处理。

[0036] 作为进一步优选的实施方式，所述步骤 c，其包括 ：

[0037] 文件云引擎对文件内容的安全性进行判断，并将返回的安全结果存储起来 ；

[0038] 毒霸 KSC 引擎对非文件内容维度的启动点安全性进行判断，并判断该安全结果是否为 KSC 高启发威胁特征，若是，则对文件云引擎返回的安全结果进行获取后，将文件云引擎返回的安全结果以及毒霸 KSC 引擎返回的安全结果一起提交给安全等级逻辑处理模块，否则将继续执行 KSC 独立流程。而文件云引擎在返回安全结果后将继续执行文件云引擎独立流程。

[0039] 作为进一步优选的实施方式，所述步骤 c 中文件云引擎返回的安全结果存储在文件云引擎结果存储器内。

[0040] 作为进一步优选的实施方式，所述步骤 c 中文件云引擎返回的安全结果包括云 2.0 安全、云 3.0 安全、云 2.0 危险、云 3.0 危险、未知这五种状态，毒霸 KSC 引擎返回的安全结果包括安全、危险、高启发威胁、未知 + 分布广度这四种状态和启动点的广度值。

[0041] 作为进一步优选的实施方式，所述安全等级逻辑处理模块中的逻辑为 ：

[0042] 如果毒霸 KSC 引擎状态 = 云 3.0 安全，则最终安全等级为安全 ；

[0043] 如果毒霸 KSC 引擎状态 = 云 2.0 安全且文件云引擎广度 < 预定阈值，则最终安全等级为可疑 ；

[0044] 如果毒霸 KSC 引擎状态 = 云 2.0 安全且文件云引擎广度 >= 预定阈值，则最终安全等级为安全 ；

[0045] 否则，其他情况最终安全等级均为威胁。

[0046] 当毒霸 KSC 引擎返回的安全结果为高启发威胁状态时，毒霸 KSC 引擎才会把该状态信息传给安全等级逻辑处理模块，并且毒霸 KSC 引擎还会将启动点的广度信息传给安全等级逻辑处理模块。而文件云引擎的每个状态都会传给安全等级逻辑处理模块。

[0047] 由此可见，本发明多维度引擎间联合判定启动点安全性的检测方法，发挥了文件云引擎和毒霸 KSC 引擎之间的最大联动，把各引擎的强势发挥出来，形成各引擎之间的联动互补，优缺互补的检测策略最终判定启动点的安全性的检测方式是更安全的。

[0048] 以上是对本发明的较佳实施例进行了具体说明，但本发明创造并不限于所述实施例，熟悉本领域的技术人员在不违背本发明精神的前提下还可以作出种种的等同变形或替换，这些等同的变形或替换均包含在本申请权利要求所限定的范围内。

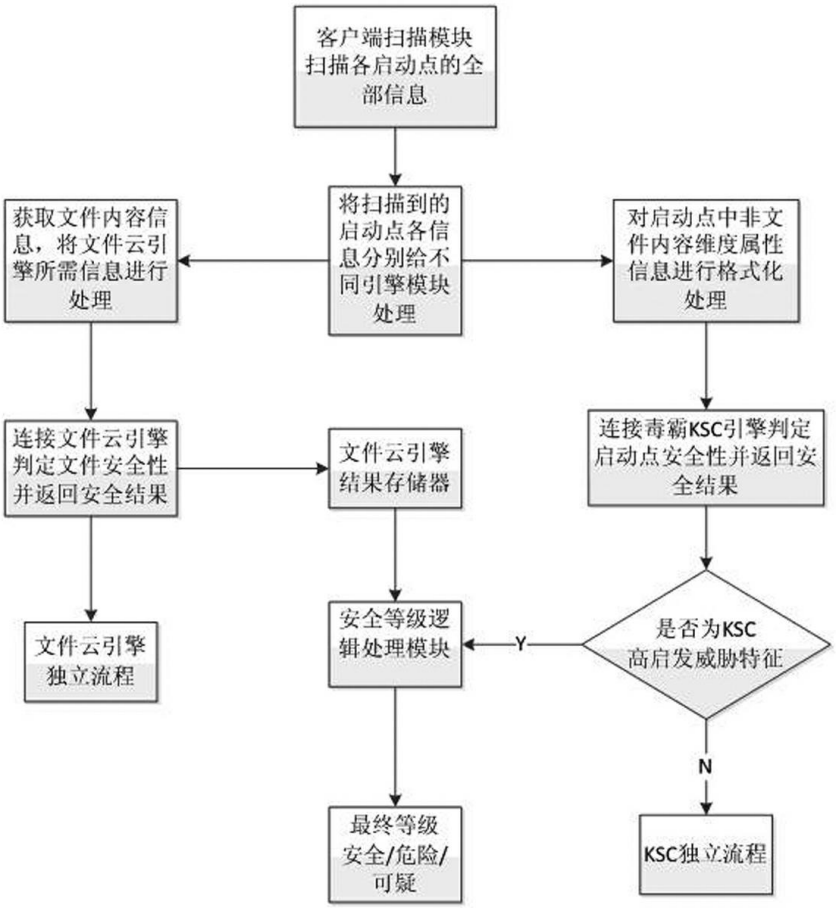

客户端扫描模块扫描各启动点的全部信息
将扫描到的启动点各信息分别给不同引擎模块处理
获取文件内容信息，将文件云引擎所需信息进行处理
对启动点中非文件内容维度属性信息进行格式化处理
连接文件云引擎判定文件安全性并返回安全结果
文件云引擎结果存储器
连接毒霸KSC引擎判定启动点安全性并返回安全结果
文件云引擎独立流程
安全等级逻辑处理模块
Y
是否为KSC高启发威胁特征
N
最终等级安全/危险/可疑
KSC独立流程

图 1