



## (12)发明专利申请

(10)申请公布号 CN 108108619 A

(43)申请公布日 2018.06.01

(21)申请号 201711483876.6

(22)申请日 2017.12.29

(71)申请人 哈尔滨安天科技股份有限公司

地址 150090 黑龙江省哈尔滨市开发区南岗集中区红旗大街162号506室内

(72)发明人 肖新光 童志明 叶佳旭 何公道

(51)Int.Cl.

G06F 21/56(2013.01)

G06F 21/64(2013.01)

H04L 9/32(2006.01)

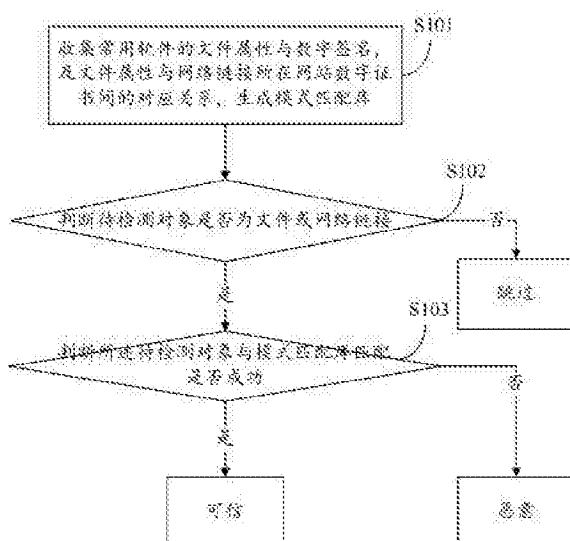
权利要求书2页 说明书5页 附图2页

(54)发明名称

基于模式匹配对应关系的文件检测方法、系统及存储介质

(57)摘要

本发明提出一种基于模式匹配对应关系的文件检测方法、系统及存储介质，本发明通过收集常用软件的文件属性与数字签名，及文件属性与网络链接所在网站数字证书间的对应关系，生成模式匹配库；判断待检测对象是否为文件或网络链接，如果是，则将所述待检测对象与模式匹配库匹配，否则跳过；若所述待检测对象与模式匹配库匹配成功，则所述待检测对象可信，否则所述待检测对象为恶意。本发明还给出相应系统及存储介质的技术方案。通过本发明方法，能够快速准确识别具有伪装及欺骗行为的文件及连接，节省了人工提取所付出的劳动力，并且快速响应。



1. 一种基于模式匹配对应关系的文件检测方法,其特征在于,包括:

收集常用软件的文件属性与数字签名,及文件属性与网络链接所在网站数字证书间的对应关系,生成模式匹配库;

判断待检测对象是否为文件或网络链接,如果是,则将所述待检测对象与模式匹配库匹配,否则跳过;

若所述待检测对象与模式匹配库匹配成功,则所述待检测对象可信,否则所述待检测对象为恶意。

2. 如权利要求1所述的方法,其特征在于,所述的判断待检测对象是否为文件或网络链接,如果是,则将所述待检测对象与模式匹配库匹配,具体为:

判断待检测对象是文件或网络链接;

如果待检测对象为文件,则提取待检测对象的文件属性及数字签名,并将其与模式匹配库匹配,若模式匹配库中存在待检测对象文件属性,且数字签名与模式匹配库中对应的数字签名相同,则判定该文件正常;若模式匹配库中存在待检测对象文件属性,且数字签名与模式匹配库中对应的数字签名不同,则判定该文件为恶意;

如果待检测对象为网络链接,则提取待检测对象的文件属性及网络链接所在网站数字证书,并将其与模式匹配库匹配,若模式匹配库中存在待检测对象文件属性,且数字证书与模式匹配库中对应的数字证书相同,则判定该网络链接正常;若模式匹配库中存在待检测对象文件属性,且数字证书与模式匹配库中对应的数字证书不同,则判定该网络链接为可疑链接。

3. 一种基于模式匹配对应关系的文件检测系统,其特征在于,包括:

模式匹配库模块,收集常用软件的文件属性与数字签名,及文件属性与网络链接所在网站数字证书间的对应关系,生成模式匹配库;

判断模块,判断待检测对象是否为文件或网络链接,如果是,则将所述待检测对象与模式匹配库匹配,否则跳过;

匹配模块,若所述待检测对象与模式匹配库匹配成功,则所述待检测对象可信,否则所述待检测对象为恶意。

4. 如权利要求3所述的系统,其特征在于,所述的判断待检测对象是否为文件或网络链接,如果是,则将所述待检测对象与模式匹配库匹配,具体为:

判断待检测对象是文件或网络链接;

如果待检测对象为文件,则提取待检测对象的文件属性及数字签名,并将其与模式匹配库匹配,若模式匹配库中存在待检测对象文件属性,且数字签名与模式匹配库中对应的数字签名相同,则判定该文件正常;若模式匹配库中存在待检测对象文件属性,且数字签名与模式匹配库中对应的数字签名不同,则判定该文件为恶意;

如果待检测对象为网络链接,则提取待检测对象的文件属性及网络链接所在网站数字证书,并将其与模式匹配库匹配,若模式匹配库中存在待检测对象文件属性,且数字证书与模式匹配库中对应的数字证书相同,则判定该网络链接正常;若模式匹配库中存在待检测对象文件属性,且数字证书与模式匹配库中对应的数字证书不同,则判定该网络链接为可疑链接。

5. 一种非临时性计算机可读存储介质,其上存储有计算机程序,其特征在于,该程序被

处理器执行时实现如权利要求1-2中任一所述的基于模式匹配对应关系的文件检测方法。

## 基于模式匹配对应关系的文件检测方法、系统及存储介质

### 技术领域

[0001] 本发明涉及信息安全技术领域,特别涉及一种基于模式匹配对应关系的文件检测方法、系统及存储介质。

### 背景技术

[0002] 如今网络上存在大量恶意软件,通过伪装成常用软件的方式,如伪装图标、伪装文件名等,达到诱使用户运行的目的。对于这类软件,目前的检测手段比较有限,多为人工提取特征等方式,虽然人工提取准确率高,但效率较低,不能实现快速响应。对于最新的启发式检测,该检测方式虽然效率高且自动化,但是准确率不够。同时无法对层出不穷的具有伪装行为的软件做到快速响应。

### 发明内容

[0003] 基于上述问题,本发明提出一种基于模式匹配对应关系的文件检测方法、系统及存储介质,通过本发明方法,解决了传统方法中效率低,响应速度慢的问题。

[0004] 本发明通过以下方法实现:

一种基于模式匹配对应关系的文件检测方法,包括:

收集常用软件的文件属性与数字签名,及文件属性与网络链接所在网站数字证书间的对应关系,生成模式匹配库;

判断待检测对象是否为文件或网络链接,如果是,则将所述待检测对象与模式匹配库匹配,否则跳过;

若所述待检测对象与模式匹配库匹配成功,则所述待检测对象可信,否则所述待检测对象为恶意。

[0005] 所述的方法中,所述的判断待检测对象是否为文件或网络链接,如果是,则将所述待检测对象与模式匹配库匹配,具体为:

判断待检测对象是文件或网络链接;

如果待检测对象为文件,则提取待检测对象的文件属性及数字签名,并将其与模式匹配库匹配,若模式匹配库中存在待检测对象文件属性,且数字签名与模式匹配库中对应的数字签名相同,则判定该文件正常;若模式匹配库中存在待检测对象文件属性,且数字签名与模式匹配库中对应的数字签名不同,则判定该文件为恶意;

如果待检测对象为网络链接,则提取待检测对象的文件属性及网络链接所在网站数字证书,并将其与模式匹配库匹配,若模式匹配库中存在待检测对象文件属性,且数字证书与模式匹配库中对应的数字证书相同,则判定该网络链接正常;若模式匹配库中存在待检测对象文件属性,且数字证书与模式匹配库中对应的数字证书不同,则判定该网络链接为可疑链接。

[0006] 本发明还提出一种基于模式匹配对应关系的文件检测系统,包括:

模式匹配库模块,收集常用软件的文件属性与数字签名,及文件属性与网络链接所在

网站数字证书间的对应关系,生成模式匹配库;

判断模块:判断待检测对象是否为文件或网络链接,如果是,则将所述待检测对象与模式匹配库匹配,否则跳过;

匹配模块,若所述待检测对象与模式匹配库匹配成功,则所述待检测对象可信,否则所述待检测对象为恶意。

[0007] 所述的系统中,所述的判断待检测对象是否为文件或网络链接,如果是,则将所述待检测对象与模式匹配库匹配,具体为:

判断待检测对象是文件或网络链接;

如果待检测对象为文件,则提取待检测对象的文件属性及数字签名,并将其与模式匹配库匹配,若模式匹配库中存在待检测对象文件属性,且数字签名与模式匹配库中对应的数字签名相同,则判定该文件正常;若模式匹配库中存在待检测对象文件属性,且数字签名与模式匹配库中对应的数字签名不同,则判定该文件为恶意;

如果待检测对象为网络链接,则提取待检测对象的文件属性及网络链接所在网站数字证书,并将其与模式匹配库匹配,若模式匹配库中存在待检测对象文件属性,且数字证书与模式匹配库中对应的数字证书相同,则判定该网络链接正常;若模式匹配库中存在待检测对象文件属性,且数字证书与模式匹配库中对应的数字证书不同,则判定该网络链接为可疑链接。

[0008] 本发明还提出一种非临时性计算机可读存储介质,其上存储有计算机程序,其特征在于,该程序被处理器执行时实现上述中任一所述的基于模式匹配对应关系的文件检测方法。

[0009] 本发明的优势在于,通过建立模式匹配库,利用文件属性和数字签名及数字证书的唯一对应关系,对比文件属性与数字签名或网络链接所在网站的数字证书,识别具有伪装和欺诈行为的文件及网络链接,能够快速准确识别具有伪装及欺骗行为的文件及连接,节省了人工提取所付出的劳动力,达到真正快速响应的结果。

## 附图说明

[0010] 为了更清楚地说明本发明或现有技术中的技术方案,下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图仅仅是本发明中记载的一些实施例,对于本领域普通技术人员来讲,在不付出创造性劳动的前提下,还可以根据这些附图获得其他的附图。

[0011] 图1为本发明基于模式匹配对应关系的文件检测方法实施例一流程图;

图2为本发明基于模式匹配对应关系的文件检测方法实施例二流程图;

图3为本发明基于模式匹配对应关系的文件检测系统结构示意图。

## 具体实施方式

[0012] 为了使本技术领域的人员更好地理解本发明实施例中的技术方案,并使本发明的上述目的、特征和优点能够更加明显易懂,下面结合附图对本发明中技术方案作进一步详细的说明。

[0013] 由于软件的数字签名具有认证功能,因此文件属性与其数字签名纸件存在对应关

系,如:Flash的安装包图标和文件名等文件属性,与Adobe公司的数字签名之间存在一一对应的关系。当用户在网络上下载Flash软件时,下载下来的软件都会伪装成Flash的文件名,但当用户点击安装时,会发现好多是下载器,广告件,甚至是恶意软件。这些具有伪装欺骗性质的软件都不具有Adobe公司的数字签名。通过这个关系,可以对这类性质的软件达到快速响应。

[0014] 另外,在网络流量测也可以通过此关系进行检测。通常情况下,用户访问的网站都有网站的证书进行认证。当用户下载文件时,检测该文件对应的网站证书是否正确,不正确的链接即可列入可疑链接范畴。

[0015] 基于上述原理,本发明提出了一种基于模式匹配对应关系的文件检测方法、系统及存储介质,通过以下方法实现:

一种基于模式匹配对应关系的文件检测方法,如图1所示,包括:

S101:收集常用软件的文件属性与数字签名,及文件属性与网络链接所在网站数字证书间的对应关系,生成模式匹配库;

S102:判断待检测对象是否为文件或网络链接,如果是,则将所述待检测对象与模式匹配库匹配,否则跳过;

S103:判断所述待检测对象与模式匹配库匹配是否成功,如果是,则所述待检测对象可信,否则所述待检测对象为恶意。

[0016] 所述的方法中,所述的判断待检测对象是否为文件或网络链接,如果是,则将所述待检测对象与模式匹配库匹配,具体为:

判断待检测对象是文件或网络链接;

如果待检测对象为文件,则提取待检测对象的文件属性及数字签名,并将其与模式匹配库匹配,若模式匹配库中存在待检测对象文件属性,且数字签名与模式匹配库中对应的数字签名相同,则判定该文件正常;若模式匹配库中存在待检测对象文件属性,且数字签名与模式匹配库中对应的数字签名不同,则判定该文件为恶意;

如果待检测对象为网络链接,则提取待检测对象的文件属性及网络链接所在网站数字证书,并将其与模式匹配库匹配,若模式匹配库中存在待检测对象文件属性,且数字证书与模式匹配库中对应的数字证书相同,则判定该网络链接正常;若模式匹配库中存在待检测对象文件属性,且数字证书与模式匹配库中对应的数字证书不同,则判定该网络链接为可疑链接。

[0017] 本发明还给出另一方法实施例二,如图2所示:

S201:收集常用软件的文件属性与数字签名,及文件属性与网络链接所在网站数字证书间的对应关系,生成格式统一的模式匹配库;

S202:判断待检测对象是文件或网络链接,如果是文件,则执行S203,如果是网络链接,则执行S205;

S203:提取待检测对象的文件属性及数字签名;

S204:将文件属性及数字签名与模式匹配库匹配,如果匹配成功,则所述待检测对象为正常文件,即在模式匹配库中存在待检测对象的文件属性,且待检测对象的数字签名也与模式匹配库中对应数字签名一致,则所述待检测对象为正常文件;否则,所述待检测对象具有伪装、欺骗行为,即在模式匹配库中存在待检测对象的文件属性,且待检测对象的数字签

名与模式匹配库中对应数字签名不一致，则所述待检测对象具有伪装、欺骗行为；

S205：提取待检测对象的文件属性及网络链接所在网站的数字证书；

S206：将文件属性及数字证书与模式匹配库匹配，如果匹配成功，则所述待检测对象为正常文件，即在模式匹配库中存在待检测对象的文件属性，且待检测对象的数字证书也与模式匹配库中对应数字证书一致，则所述待检测对象为正常链接；否则，所述待检测对象为可疑链接，即在模式匹配库中存在待检测对象的文件属性，且待检测对象的数字证书与模式匹配库中对应数字证书不一致，则所述待检测对象为可疑链接。

[0018] 本发明还提出一种基于模式匹配对应关系的文件检测系统，如图3所示，包括：

模式匹配库模块301，收集常用软件的文件属性与数字签名，及文件属性与网络链接所在网站数字证书间的对应关系，生成模式匹配库；

判断模块302，判断待检测对象是否为文件或网络链接，如果是，则将所述待检测对象与模式匹配库匹配，否则跳过；

匹配模块303，若所述待检测对象与模式匹配库匹配成功，则所述待检测对象可信，否则所述待检测对象为恶意。

[0019] 所述的系统中，所述的判断待检测对象是否为文件或网络链接，如果是，则将所述待检测对象与模式匹配库匹配，具体为：

判断待检测对象是文件或网络链接；

如果待检测对象为文件，则提取待检测对象的文件属性及数字签名，并将其与模式匹配库匹配，若模式匹配库中存在待检测对象文件属性，且数字签名与模式匹配库中对应的数字签名相同，则判定该文件正常；若模式匹配库中存在待检测对象文件属性，且数字签名与模式匹配库中对应的数字签名不同，则判定该文件为恶意；

如果待检测对象为网络链接，则提取待检测对象的文件属性及网络链接所在网站数字证书，并将其与模式匹配库匹配，若模式匹配库中存在待检测对象文件属性，且数字证书与模式匹配库中对应的数字证书相同，则判定该网络链接正常；若模式匹配库中存在待检测对象文件属性，且数字证书与模式匹配库中对应的数字证书不同，则判定该网络链接为可疑链接。

[0020] 本发明还提出一种非临时性计算机可读存储介质，其上存储有计算机程序，其特征在于，该程序被处理器执行时实现上述中任一所述的基于模式匹配对应关系的文件检测方法。

[0021] 本发明的优势在于，通过建立模式匹配库，利用文件属性和数字签名及数字证书的唯一对应关系，对比文件属性与数字签名或网络链接所在网站的数字证书，识别具有伪装和欺诈行为的文件及网络链接，能够快速准确识别具有伪装及欺骗行为的文件及连接，节省了人工提取所付出的劳动力，达到真正快速响应的结果。

[0022] 通过以上的实施方式的描述可知，本领域的技术人员可以清楚地了解到本发明可借助软件加必需的通用硬件平台的方式来实现。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品可以存储在存储介质中，如ROM/RAM、磁碟、光盘等，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本发明各个实施例或者实施例的某些部分所述的方法。

[0023] 本说明书中的各个实施例均采用递进的方式描述,各个实施例之间相同相似的部分互相参见即可,每个实施例重点说明的都是与其他实施例的不同之处。尤其,对于系统实施例而言,由于其基本相似于方法实施例,所以描述的比较简单,相关之处参见方法实施例的部分说明即可。

[0024] 虽然通过实施例描绘了本发明,本领域普通技术人员知道,本发明有许多变形和变化而不脱离本发明的精神,希望所附的权利要求包括这些变形和变化而不脱离本发明的精神。

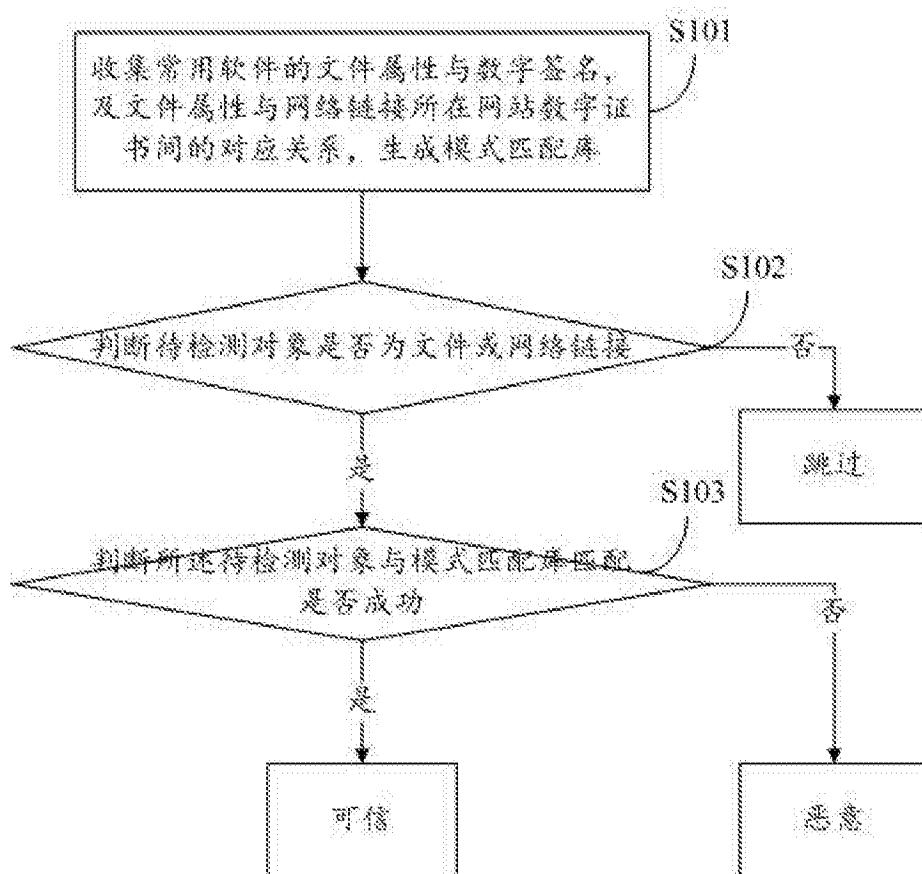


图1

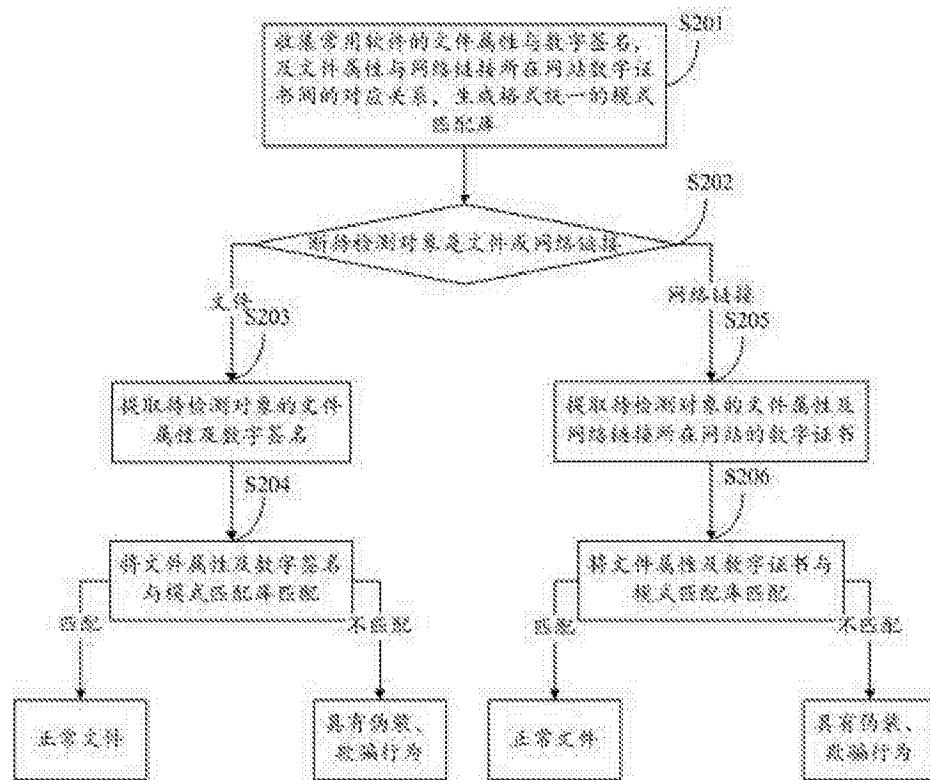


图2

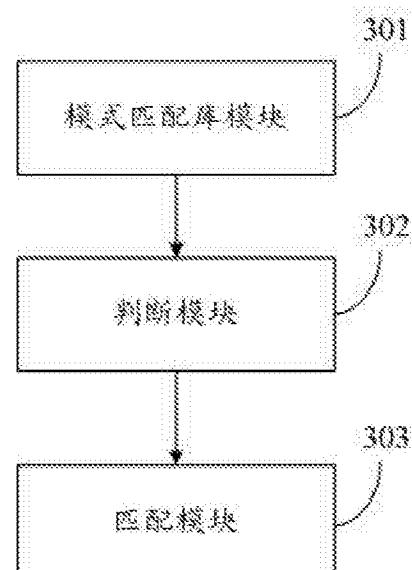


图3