



(12) 发明专利申请

(10) 申请公布号 CN 103905421 A

(43) 申请公布日 2014. 07. 02

(21) 申请号 201310689748. 2

(22) 申请日 2013. 12. 17

(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

(72) 发明人 童志明 沈长伟 张栗伟

(51) Int. Cl.

H04L 29/06 (2006. 01)

G06F 17/30 (2006. 01)

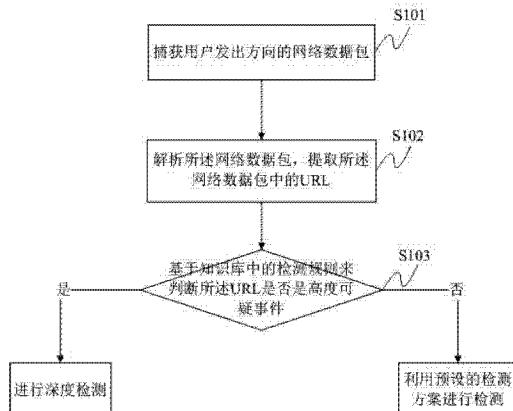
权利要求书1页 说明书3页 附图1页

(54) 发明名称

一种基于 URL 异构性的可疑事件检测方法及  
系统

(57) 摘要

本发明公开了一种基于 URL 异构性的可疑事件检测方法及系统,首先,捕获用户发出方向的网络数据包;解析所述网络数据包,提取所述网络数据包中的 URL;基于知识库中的检测规则来判断所述 URL 是否是高度可疑事件,若是,则进行深度检测,否则利用预设的检测方案进行检测;所述检测规则根据需要添加或删除,包括:判断所述 URL 请求的服务器端口是否为系统保留端口,若是,则是安全事件,否则是高度可疑事件;判断所述 URL 的域名是否是具有实际意义的词汇,若是,则是安全事件,否则是高度可疑事件。解决了传统检测方法对于已知恶意的 URL 有效,对于未知的或者未捕获的 URL 无能为力的问题。



1. 一种基于 URL 异构性的可疑事件检测方法,其特征在于,包括 :

捕获用户发出方向的网络数据包 ;

解析所述网络数据包,提取所述网络数据包中的 URL ;

基于知识库中的检测规则来判断所述 URL 是否是高度可疑事件,若是,则进行深度检测,否则利用预设的检测方案进行检测 ;

所述检测规则根据需要添加或删除,包括 :

判断所述 URL 请求的服务器端口是否为系统保留端口,若是,则是安全事件,否则是高度可疑事件 ;

判断所述 URL 的域名是否是具有实际意义的词汇,若是,则是安全事件,否则是高度可疑事件。

2. 如权利要求1所述的方法,其特征在于,若判断所述URL请求的服务器端口是系统保留端口,则继续判断所述URL请求是否与端口所对应的协议一致,若是,则是安全事件,否则是高度可疑事件。

3. 一种基于 URL 异构性的可疑事件检测系统,其特征在于,包括 :

数据包捕获模块,用于捕获用户发出方向的网络数据包 ;

URL 提取模块,用于解析所述网络数据包,提取所述网络数据包中的 URL ;

判定模块,用于基于知识库中的检测规则来判定所述 URL 是否是高度可疑事件,若是,则进行深度检测,否则利用预设的检测方案进行检测 ;

知识库,用于存储检测规则,所述检测规则根据需要添加或删除,包括 :

判断所述 URL 请求的服务器端口是否为系统保留端口,若是,则是安全事件,否则是高度可疑事件 ;

判断所述 URL 的域名是否是具有实际意义的词汇,若是,则是安全事件,否则是高度可疑事件。

4. 如权利要求3所述的系统,其特征在于,若判断所述URL请求的服务器端口是系统保留端口,则继续判断所述URL请求是否与端口所对应的协议一致,若是,则是安全事件,否则是高度可疑事件。

## 一种基于 URL 异构性的可疑事件检测方法及系统

### 技术领域

[0001] 本发明涉及网络安全技术领域，尤其涉及一种基于 URL 异构性的可疑事件检测方法及系统。

### 背景技术

[0002] 用来浏览网站的 web 浏览器已经从展示内容发展为一个可执行分布式应用程序的环境。为了能更好的展示网站的各种功能，浏览器已经从原来的静态角色转变成了可以动态运行客户端程序的操作系统，同时也给用户带来了更大的安全隐患。

[0003] 传统恶意程序的检测方法多是基于特征码进行检测，对于 URL 进行检测的方法是通过已知捕获的恶意 URL 进行匹配，但是这种方式对于未知的恶意 URL 基本无效，并且其反应速度也远远落后于恶意程序发展及转化的速度。

### 发明内容

[0004] 针对上述技术问题，本发明提供了一种基于 URL 异构性的可疑事件检测方法及系统，该发明通过知识库中的检测规则来检测 URL 是否是高度可疑事件，并及时处理和响应。由于知识库中的检测规则是可以根据形势和需要补充或者替换，所以便于维护，并且由于本发明所提供的技术方案不依赖于已知恶意 URL 的特征提取，所以其对于未知的恶意 URL 有很好的检出效果。

[0005] 本发明采用如下方法来实现：一种基于 URL 异构性的可疑事件检测方法，包括：

捕获用户发出方向的网络数据包；

解析所述网络数据包，提取所述网络数据包中的 URL；

基于知识库中的检测规则来判断所述 URL 是否是高度可疑事件，若是，则进行深度检测，否则利用预设的检测方案进行检测；

所述检测规则根据需要添加或删除，包括：

判断所述 URL 请求的服务器端口是否为系统保留端口，若是，则是安全事件，否则是高度可疑事件；其中，所述系统保留端口小于等于 1024；通常正常的网络服务都是使用系统保留端口，例如：HTTP 的 80 端口、FTP 的 22 端口等。恶意程序由于很多条件限制，例如为了逃避检测，所以很少使用系统保留端口；

判断所述 URL 的域名是否是具有实际意义的词汇，若是，则是安全事件，否则是高度可疑事件。因为正常的网络服务一般都会选择一个具有实际意义的单词、拼音或者已知域名等作为域名。恶意程序为了隐藏自己需求等原因，可能需要使用没有任何实际意义的域名。

[0006] 其中，所述检测规则是可以不断完善的，能够根据形势或者需要添加新的检测规则，或者删除不再有效地检测规则。

[0007] 进一步地，若判断所述 URL 请求的服务器端口是系统保留端口，则继续判断所述 URL 请求是否与端口所对应的协议一致，若是，则是安全事件，否则是高度可疑事件。

[0008] 本发明采用如下系统来实现：一种基于 URL 异构性的可疑事件检测系统，包括：

数据包捕获模块,用于捕获用户发出方向的网络数据包;

URL 提取模块,用于解析所述网络数据包,提取所述网络数据包中的 URL;

判定模块,用于基于知识库中的检测规则来判定所述 URL 是否是高度可疑事件,若是,则进行深度检测,否则利用预设的检测方案进行检测;

知识库,用于存储检测规则,所述检测规则根据需要添加或删除,包括:

判断所述 URL 请求的服务器端口是否为系统保留端口,若是,则是安全事件,否则是高度可疑事件;其中,所述系统保留端口小于等于 1024;通常正常的网络服务都是使用系统保留端口,例如:HTTP 的 80 端口、FTP 的 22 端口等。恶意程序由于很多条件限制,例如为了逃避检测,所以很少使用系统保留端口;

判断所述 URL 的域名是否是具有实际意义的词汇,若是,则是安全事件,否则是高度可疑事件。因为正常的网络服务一般都会选择一个具有实际意义的单词、拼音或者已知的域名等作为域名。恶意程序为了隐藏自己需求等原因,可能需要使用没有任何实际意义的域名。

[0009] 其中,所述知识库是可以不断完善的,能够根据形势或者需要添加新的检测规则,或者删除不再有效地检测规则。

[0010] 进一步地,若判断所述 URL 请求的服务器端口是系统保留端口,则继续判断所述 URL 请求是否与端口所对应的协议一致,若是,则是安全事件,否则是高度可疑事件。

[0011] 综上所述,本发明提供了一种基于 URL 异构性的可疑事件检测方法及系统,利用恶意程序通常都会主动与控制端进行网络通信的特点,本发明所述技术方案通过监控用户发出方向的网络数据包,并解析出 URL,基于预设的检测规则检测所述 URL 请求是否是高度可疑事件,并根据检测结果进行后续处理。由于本技术方案没有使用已知恶意 URL 特征进行检测,并且其使用的检测规则可以根据需要灵活添加或者删除,所以其可以有效地检出未知恶意 URL。

## 附图说明

[0012] 为了更清楚地说明本发明的技术方案,下面将对实施例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。

[0013] 图 1 为本发明提供的一种基于 URL 异构性的可疑事件检测方法流程图;

图 2 为本发明提供的一种基于 URL 异构性的可疑事件检测系统结构图。

## 具体实施方式

[0014] 本发明给出了一种基于 URL 异构性的可疑事件检测方法及系统,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:

本发明首先提供了一种基于 URL 异构性的可疑事件检测方法,如图 1 所示,包括:

S101 捕获用户发出方向的网络数据包;

S102 解析所述网络数据包,提取所述网络数据包中的 URL;

S103 基于知识库中的检测规则来判断所述 URL 是否是高度可疑事件,若是,则进行深

度检测，否则利用预设的检测方案进行检测；

所述检测规则根据需要添加或删除，包括：

判断所述 URL 请求的服务器端口是否为系统保留端口，若是，则是安全事件，否则是高度可疑事件；

判断所述 URL 的域名是否是具有实际意义的词汇，若是，则是安全事件，否则是高度可疑事件。

[0015] 优选地，若判断所述 URL 请求的服务器端口是系统保留端口，则继续判断所述 URL 请求是否与端口所对应的协议一致，若是，则是安全事件，否则是高度可疑事件。

[0016] 本发明还提供了一种基于 URL 异构性的可疑事件检测系统，如图 2 所示，包括：

数据包捕获模块 201，用于捕获用户发出方向的网络数据包；

URL 提取模块 202，用于解析所述网络数据包，提取所述网络数据包中的 URL；

判定模块 203，用于基于知识库中的检测规则来判定所述 URL 是否是高度可疑事件，若是，则进行深度检测，否则利用预设的检测方案进行检测；

知识库 204，用于存储检测规则，所述检测规则根据需要添加或删除，包括：

判断所述 URL 请求的服务器端口是否为系统保留端口，若是，则是安全事件，否则是高度可疑事件；

判断所述 URL 的域名是否是具有实际意义的词汇，若是，则是安全事件，否则是高度可疑事件。

[0017] 优选地，若判断所述 URL 请求的服务器端口是系统保留端口，则继续判断所述 URL 请求是否与端口所对应的协议一致，若是，则是安全事件，否则是高度可疑事件。

[0018] 如上所述，本发明给出了一种基于 URL 异构性的可疑事件检测方法及系统的具体实施例，其与传统方法的区别在于，目前多数恶意 URL 的检测方法是基于已知恶意 URL 的特征提取，基于特征对于 URL 进行扫描，并判定是否是恶意 URL。但是现有技术的检测效果依赖于特征库的大小或者更新速度，并且对于未知恶意 URL 基本没有检出能力。而本发明所述的技术方案是利用恶意 URL 的通信特点，监控并获取向外发出的请求网络数据包，并提取 URL，基于预先定义的知识库中的检测规则，对于 URL 进行检测并判断其是否是恶意 URL，基于判定结果进行后续处理。由于本发明所述技术方案不依赖于已知特征，并且其使用的知识库是可以根据形势需要进行维护的，可以向内添加或者删除检测规则，因此对于未知的或者未捕获的恶意 URL 有更好的检测效果。

[0019] 以上实施例用以说明而非限制本发明的技术方案。不脱离本发明精神和范围的任何修改或局部替换，均应涵盖在本发明的权利要求范围当中。

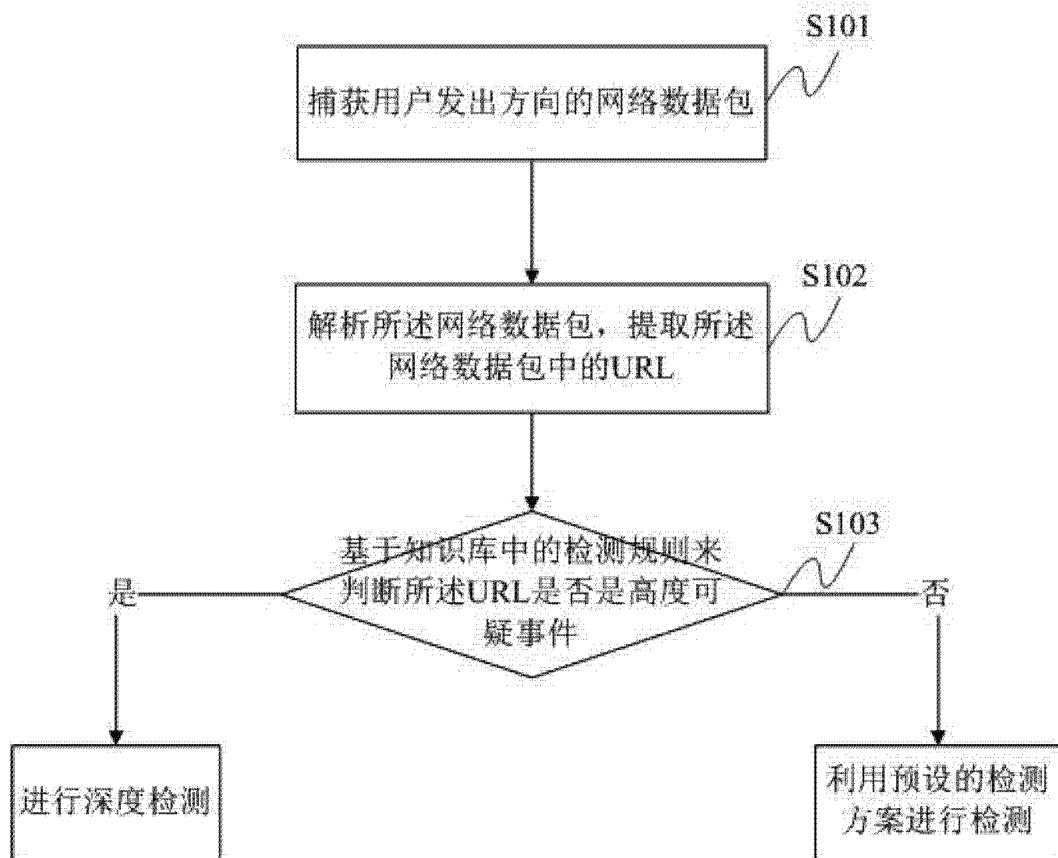


图 1

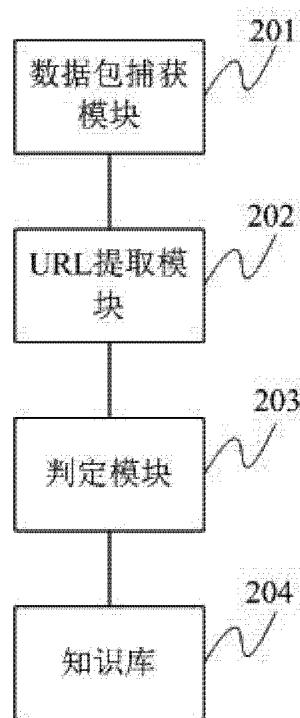


图 2