文章编号: 1009 - 2552(2012)02 - 0149 - 03 中图分类号: TP393.08 文献标识码: A

基于行为分析的木马检测

徐旭旭，薛 质，吴 刚

(上海交通大学软件学院，上海 200240)

摘 要: 首先介绍了特洛伊木马的基本概念，其利用的基本技术，再介绍了常用的木马检测方法。阐述了木马检测的现状和发展趋势。分析并归纳了木马在安装阶段的行为特征，以此提出基于行为分析的木马检测方法。

关键词: 木马; 行为特征; 安装; 策略; 倾向

Detection of Trojan Horse based on behavior analysis

XU Xu-xu, XUE Zhi, WU Gang

(School of Software, Shanghai Jiaotong University, Shanghai 200240, China)

Abstract: This paper first introduced the basic conceptions about Trojan Horse and basic technologies of Trojan Horse, and then it introduced the common methods of Trojan Horse detection . And it expounds the current research condition and development trend of Trojan Horse detection. It analyzes and summarizes the behavioral characteristics of their installation, and puts forward an anti-trojan strategy based on behavior analysis.

Key words: trojan horset; behavioral characteristics; installtion; strategy; trend

0 引言

随着计算机网络的不断发展，全球信息化已成为人类发展的大趋势。网络信息系统已经成为社会，政府，企业，学校，科研院所，军队的重要基础设施和交流的工具，其作用日趋重要。但是，出现了各种黑客攻击和网络攻击手段，而木马攻击以其隐蔽性强，攻击范围比较广，危害比较大等特点成为了最为常见的网络攻击技术之一，对网络安全造成了非常大的威胁。网络安全迫切需要有效的木马防范技术。

1 特洛伊木马概述

1.1 特洛伊木马的定义

特洛伊木马是指附着在应用程序中或者单独存在的一些恶意的程序，利用网络远程响应网络另一端的控制程序，实现对感染木马程序的计算机控制。控制者可以控制被秘密植入木马的计算机的一切动作和资源，是恶意攻击者进行窃取信息等的工具。木马程序以 C/S 模式为主，木马服务器的端程序在被控制的主机上运行，客户端来控制。

1.2 特洛伊木马的种类

后门型木马: 这种木马在目标系统中会打开一个特定的后门以便攻击者进入此系统。后门类型主要有: Ftp Server, Proxy Server, HTTP Server, Telnet Server 等。

远程控制型木马: 这种木马是目前最流行的木马，由控制端和服务端两部分组成。这类木马的服务端必须得先植入目标系统并且运行，接着将控制端连接到服务端。

信息收集型木马: 这种木马会记录或收集系统各种重要信息，比如获取登录口令，MSN 密码，邮箱密码，也可以记录系统操作，键盘按键情况，然后发送给特定的攻击者。

系统配置修改型: 这种木马会修改系统配置。比如修改注册表使磁盘共享随后关闭。

1.3 特洛伊木马的隐蔽技术

特洛伊木马的隐蔽性是指木马设计者为了防止

收稿日期: 2011 - 08 - 25

作者简介: 徐旭旭(1983 -)，男，硕士，研究方向为软件工程。

木马程序被发现而采取的各种隐蔽手段。即使被发现,木马也会因为无法具体定位而无法清除掉。木马在被植入目标系统的运行空间中,必须以进程,线程的运行形势。在用户角度可以观察到进程,而线程是观察不到的。木马可以隐蔽自己的 运行形式来防止目标系统的用户管理员发现。比如可以在自身植入目标系统后生成 DLL 文件,把其主要的完成恶意操作或者通信功能代码放在 DLL 中,采用各种方法把 DLL 插入其他进程执行。这个时候插入的木马 DLL 以线程形式运行在其他进程中。有的木马启动后会在远程进程中创建一个线程将恶意操作代码拷贝到创建的远程线程中运行。

2 常用木马检测方法

常用的按行为特征分类的木马检测方法有: 基于静态特征的木马检测方法和基于动态行为的木马检测方法。

2.1 基于静态特征的木马检测方法

木马静态特征归类如下:

(1) 在目标系统中运行时进程的名称。

(2) 在目标系统中生成的文件及木马原始文件的特征字符串。

(3) 在目标系统中具体的启动加载方式。

(4) 在目标系统中的生成文件名,文件大小及所在目录。

(5) 打开的固定的 TCP/UDP 端口。

2.2 基于动态行为特征的木马检测

正在不断发展壮大的木马隐蔽技术使得木马在被植入的系统中越来越难以发现。基于静态特征的木马检测技术检测已知木马的各种隐蔽和变化能力已经严重不足,并且基本无法应对未知的木马。

而基于动态行为分析的木马检测方法控制木马的隐蔽,恶意操作,植入等行为的所需要的各种资源条件,可以监控木马的通信,启动的隐蔽行为和恶意操作,以及运行行为来对木马进行检测和防范的。

2.3 木马检测的趋势

现有的木马检方式略有两种:

(1) 通过监控发现网络通信异常,阻断木马的网络通信。

采用这种方式的有防火墙,入侵检测,它们对通信端口和网络连接做严格的限制和严密的监控。入侵检测还能自动探测网络流量中潜在的入侵和攻击。

但是,目前有许多的木马趋向于采用无连接的网络通信协议,同时采取特殊的技术使通信端口很难被发现,有的甚至没有端口通信,于此同时又限制了通信流量,所以使用该方法已经越来越难将侧和阻断木马通信。

(2) 检查木马特征码文件来判断木马。

采用检测特征码的方式有特征码静态扫描,虚拟机和实时监控。

这种方式无法检测特征码没有包含于特征库中的木马,即使是已知木马,也可以通过加壳等技术避免被检测到,使得木马服务器有机会进行与客户端的通信,带来信息邪路,系统破坏等损失。另外由于新木马及各类木马变种产生的速度非常快,特征码数量也循迅速增加,试用这种方式必然需要非常大的时间开销,使得检测效率不断下降。

为克服这些缺陷,研究人员从行为的角度考虑应对方法,即行为分析: 根据程序行为特征判断其是否可疑。

3 基于行为分析的木马检测

木马入侵计算机过程有三个阶段: 投放,运行和安装木马服务器,木马服务器与木马客户端的通信。

选择在木马安装阶段拦截与查杀木马。因为木马在通信阶段表现的行为主要是接受和发送数据,这些行为与许多正常网络通信程序一致,并不适合作为区分木马的行为特征。木马在安装阶段具有显著不同于一般正常程序的行为特征,容易辨别。木马行为作用的主要对象是木马程序本身,易于获取木马程序的信息和定位木马,并将其清除。也及早保护系统注册表,系统文件等不被破坏,这样避免了清除木马的同时再对这些文件进行修复。

3.1 木马在安装阶段的行为特征

木马安装有 2 个步骤: 隐藏木马程序和木马服务器自启动设置,以便木马服务器在计算机每次开机或者重启时都自动运行。

木马行为及行为作用的对象归纳如表 1 所示。

表 1 木马安装阶段行为特征

步骤	实现途径	木马行为	作用对象
隐藏木马程序	将木马程序拷贝到系统目录	拷贝文件	木马程序,系统目录路径
木马服务器自启动设置	修改注册表	打开,读写关闭注册表项	木马程序的路径,注册表
	修改系统文件	打开,读写,关闭文件	木马程序路径,系统文件
	木马服务器拷贝到自启动目录	拷贝文件	木马程序,自启动目录路径
	拷贝 autorun.inf 文件至某根目录	拷贝文件	文件 autorun.inf,某根目录路径
	木马服务器注册为系统服务	注册系统服务	木马程序路径

3.2 API 钩子技术的应用

钩子,是 Windows 消息处理机制的一个平台,应用程序可以在上面设置子程以监视指定窗口的某种

消息，而且所监视的窗口可以是其他进程所创建的。当消息到达后，在目标窗口处理函数之前处理它。钩子机制允许应用程序截获处理 Windows 消息或特定事件。

钩子是一个处理消息的程序段，通过系统调用，把它挂入系统。每当特定的消息发出，在没有到达目的窗口前，钩子程序就先捕获该消息，亦即钩子函数先得到控制权。这时钩子函数即可以加工处理该消息，也可以不作处理而继续传递该消息，还可以强制结束消息的传递。

为了能够拦截木马，可以拦截木马上述行为表现的不同的 API 调用。

钩子能够作用于系统中所有的进程和线程。预先定义一个钩子函数，安装针对某个 API 调用的钩子，就可以在真正 API 调用发生前，先调用钩子函数。

3.3 木马检测框架

(1) 木马行为特征库。

木马行为特征库存储了行为作用对象和关于行为描述信息，API 名称。

(2) 注册表保护模块。

拦截所有修改注册表的行为，同时报警。因为修改注册表的程序比较少，用户自身也很少会去修改注册表，所以当注册表发生修改时，很有可能是木马所为。

(3) 系统服务保护模块。

系统服务保护模块会拦截所有程序注册系统服务的行为，一般软件是很少会去注册系统服务保护模块的。

(4) 当行为对象可被木马用来实现隐藏或者自启动时，会被拦截，并报警。

整个模块如图 1 所示。

3.4 本木马检测方法的特点

这个检测方法能停止木马的安装，保护注册表系统文件不被破坏，同时可以在停止木马后继进行网络监控做不到的查杀木马。木马安装阶段的程序隐蔽和自启动设置实现途径有限，所以大量木马在这个阶段的行为具有非常大的相似性，甚至相同。木马的行为特征库比较稳定，变化频率较小。木马的行为如果包含于现有的行为特征库中，就会被拦截。因为发现新的隐藏和自启动设置途径有很大的技术难度，木马常常会使用已知途径中的一种或者几种，也就是说其行为特征一般是已知的，所以已被本方法成功拦截查杀。而且有些木马是隐藏通信端口和无连接的的，网络监控较难发现，却可以根据行为特征轻易检测出来。

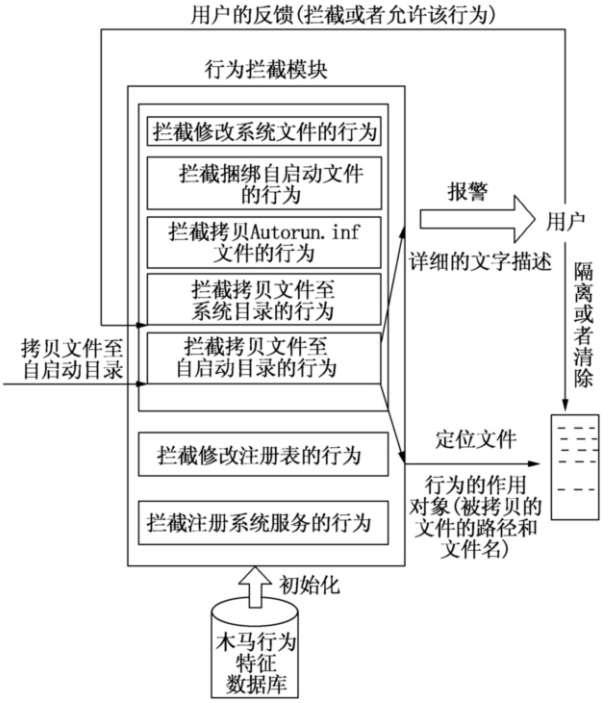

图 1 木马检测模块

4 结束语

木马攻击技术发展至今，木马植入方式，隐蔽技术发生了巨大变化。随着互联网的广泛应用越来越多的新木马会泛滥起来，给网络安全构成极大的威胁。基于行为分析的木马检测方法能够较容易地识破木马的各种检测对抗技术，对各种未知的木马也有比较好的防范能力，是一种较为可靠的木马检测方法。

但是随着技术的发展，木马制作者已经开始将木马技术继续发展，木马朝着功能多样化，嵌入内核级隐蔽，嵌入应用级远程控制的方向发展。木马会与病毒结合起来产生新的针对系统漏洞的复合物会以更快的传播方式对网络安全构成更大的威胁和破坏。

攻与防永远是网络安全领域中恒久不变的主题。能够深入了解木马如何展开攻击行动，对于更好地实施网络安全保障具有很好的借鉴意义。

参 考 文 献:

[1] Haykin S Neural Networks – A Comprehensive Foundation [M]. 机械工业出版社，2004.

[2] 戴敏. 基于文件静态信息的木马检测模型 [J]. 计算工程，2003.

[3] 李进，李伟. Windwos 9X/NT 注册表技术内幕 [M]. 清华大学出版社，2000.

[4] Jeffery Richter. Programming Applicatiions for Microsoft Windows [M]. 4th ed.

[5] LYMAN J. In search of the world's costliest computer virus [Z]. 2008.

责任编辑: 刘新影