西北大学学报(自然科学版)
2006年12月,第36卷第6期, Dec.,2006, Vol.36, No.6
Journal of Northwest University (Natural Science Edition)
JNWU

基于SPI技术漏洞的新型木马的防范方法

贺小伟[1],余景景[2],王 森[3]

(1.西北大学 信息科学与技术学院,陕西 西安 710069;2.陕西师范大学 物理学与信息技术学院,陕西 西安 710062;
3.西安交通大学 电子与信息工程学院,陕西 西安 710049)

摘要:目的 防范基于SPI技术漏洞的新型木马。**方法** 从SPI技术原理出发分析新型木马利用SPI技术实现隐藏的机制,找出一种新型木马的检测和清除方法。**结果** 提出了一套完整的针对基于SPI技术的新型木马的防御方案,并详细描述了其实现。**结论** 这种确实可行的周期比较法,可以对新型木马实施半自动清除。

关 键 词:服务提供者接口技术;新型木马;查杀木马
中图分类号:TP393 **文献标识码:**A **文章编号:**1000-274X(2006)06-0907-04

随着Winsock 2的新特性SPI技术的出现,用户可以自己开发服务提供者,提高网络管理的灵活性。但是,这项新技术无需授权认证就可以安装服务提供者,SPI技术的这种漏洞也为各种基于客户服务器方式的远程控制程序如特洛伊木马等实现其隐蔽性提供了基础。现在互联网上已经出现了基于SPI技术和远程线程技术的新型木马理论[1],虽然目前还没有公布这类新型木马,但这已经对网络安全提出了很大的挑战。本文介绍了SPI技术的原理以及新型木马利用SPI技术实现隐藏的机制,进一步结合Windows内核技术和Windows网络技术提出了一种确实可行的周期比较法,可以对该新型木马实施半自动清除。

1 基于SPI漏洞的木马隐藏技术分析

木马程序技术发展至今,已经经历了4代。从端口监听的服务型木马到现在的反弹式木马,木马程序的隐藏手段也从修改注册表发展为目前最新的通过SPI技术与远程线程技术的结合,隐藏手段越来越高明。

1.1 传统木马的启动和隐蔽方式

木马程序总会想尽一切办法隐藏自己,让用户在任务栏和任务管理器中看不到它们。传统的木马程序的启动方式,最常用的包括加入系统启动项、在Win.ini或Winstart.bat中启动、集成到程序中、修改文件关联、捆绑文件、设置在超级链接中等。针对这些传统的木马启动方式,随着网络安全技术的发展,越来越多的工具可以帮助用户自动清除这些木马。将目前比较流行的远程线程技术和传统木马的启动方式相结合,在目前的杀毒软件面前也是无所作为的,因此木马研究者们就更迫切地寻找一种更隐蔽的启动方法。

1.2 SPI技术及其优势

为了有效对抗目前的木马检测方法,有人提出了结合SPI技术与远程线程技术实现的木马原理[1],其核心思想是利用SPI实现隐藏。

服务提供者接口(SPI)是Winsock 2的一个新特性,是为编写服务提供者的人员提供的。Winsock 2中使用的服务提供者有两类:基础服务提供者和分层服务提供者。基础服务提供者执行网络传输协议,完成网络数据的实际交换;分层服务提供者只负责执行高级的自定义通信功能,并依赖基础服务提供者完成数据交换[2]。

下面详细分析一下使用这种技术隐藏木马的原理。首先分析网络应用程序的执行过程,当网络应用程序调用WSASocket函数创建套接字时,会返回3个参数:地址族,套接字类型和协议,Winsock 2提供的WS2_32.DLL利用这3个参数决定是由哪一个类型的传输服务提供者来实现本应用程序的功

收稿日期:2005-07-11
作者简介:贺小伟(1977—),男,陕西米脂人,西北大学助教,从事计算机网络与分布式系统研究。

能,并完成 API 函数到 SPI 函数的映射。在 WS2_32.DLL 匹配过程中,会按照顺序遍历系统服务提供者库,选择第一个匹配的传输服务提供者,并把传输服务提供者对应的动态链接库(DLL)加载到内存中[3]。

基于 SPI 的木马中使用的是分层传输服务提供者,在该分层传输服务提供者中不定义任何高级的通信功能,只是完成对木马进程的启动。为了使传输服务提供者的动态链接库被 WS2_32.DLL 自动调用,必须安装用户的传输服务提供者,并且把用户的传输服务提供者设置为系统默认。这样它就会被多个网络服务加载,通常在系统关闭时,系统网络服务才会结束,所以这样的木马程序同样可以在系统运行时保持激活状态。

2 基于 SPI 漏洞木马实现的技术细节

上面介绍了基于 SPI 技术实现木马安装启动的思路,下面就在 Windows 2003 系统下实现具体如何利用 SPI 技术,做些详细分析讨论,为下一步如何防范做铺垫。

首先,利用 Microsoft 在 MSDN SDK 中提供的工具 Sporder.exe,列出在安装传输服务提供者之前系统已安装的所有服务提供者,如图 1 所示。

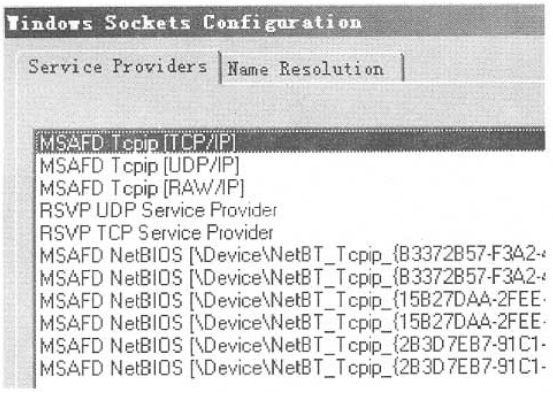

图 1 系统默认安装的服务提供者

Fig. 1 Default service providers installed by system

接下来安装传输服务提供者,安装过程主要分为以下 3 个步骤:安装分层服务提供者,安装链式提供者和对服务提供者排序。

2.1 安装分层服务提供者

要安装分层式服务提供者,需要定义两个 WSAPROTO_INFOW 结构类型的变量,一个代表分层提供者,一个代表协议链。调用 WSCEnumProtocols()函数,可以获得现有服务提供者的目录条目结构,再使用 memcpy()函数完成新变量的初始化。然后再设置分层服务提供者的协议类型(0 表示分层协议,1 表示基础协议,>1 表示协议链),惟一的 UID,名称等。完成后就可以使用 WSCInstallProvider()函数安装分层提供者的目录条目,新的分层提供者(Test ip Layered)被安装在目录的最末,如图 2 所示。

2.2 安装链式提供者

首先要通过 WSCEnumProtocols()列举出所有的目录条目,从中获得要安装的分层提供者的结构目录 ID,和与分层提供者相关的系统基础提供者的结构目录 ID。利用这两个 ID 号设置该协议链目录条目,通过该条目使安装的分层提供者与基础提供者链接起来。链接成功后通过 WSCInstallProvider()安装这个链式提供者。安装后的链式提供者(Test over MSAFD Tcpip [UDP/IP])也被安装在目录的最末。为了设置为系统默认的服务提供者,必须进行下一步排序。

2.3 提供者重排序

在安装一个新的服务提供者后,该目录条目会自动成为数据库的最末一个条目。因此,要想该服务提供者成为默认的提供者就必须对提供者进行重新排序。这个目标可以通过先定义一个利用目录 ID 组成的数组 Catalog,然后在数组 Catalog 中按照用户的要求排好序,再通过调用 WSCWriteProviderOrder() 函数来完成对提供者序列进行重排。执行排序操作后,链式提供者(Test over MSAFD Tcpip [UDP/IP])从最末端上移到了最顶端,如图 2 所示。

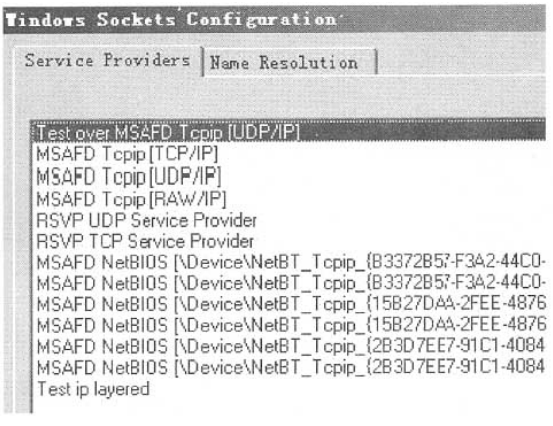

图 2 安装 SPI 木马后的系统服务提供者

Fig. 2 Servica providers after the SPI based Trojan horse was installed

3　防范基于 SPI 漏洞木马的实现方法

孙子兵法曰:“知己知彼,百战不殆”。只有对一种攻击手段的原理和实现方法分析透彻,才能够设计出行之有效的防范策略和实现方法。

3.1　防范基于 SPI 漏洞木马的实现方法

通过研究分析基于 SPI 技术的新型木马的具体实现流程,可以总结出这种新型木马利用 SPI 技术实现隐藏的两大技术特点。①必须安装传输服务提供者。传输服务提供者的安装是通过调用 WSCInstallProvider( )函数,将其安装到系统的数据库中;②必须对服务提供者数据库重排序。木马程序安装完传输服务提供者后,默认是添加到提供者数据库的最末端,所以必须利用 SPI 提供的函数 WSCWriteProviderOrder( )重新排序,让所安装的服务提供者排在库首,才能被系统自动加载。

针对以上分析的两点特性,设想如果能够实时监控 Winsock 2 的服务提供者数据库,在执行对该库的任何插入、修改、删除操作前都进行有效性认证,那就可以抵御非法安装服务提供者;另外,提供者数据库的重新排序,最终目的是让木马程序安装的协议链在库首,所以只要我们监控库首记录,就可以防御异常的对数据库的重排序。

根据以上的分析,得出要检测基于 SPI 的新型木马的关键技术就是监视 Winsock 提供者数据库,鉴于微软提供的 SPI 函数中没有对提供者数据库的相应有效性认证功能。本文采用了一种可行的周期比较法实现了对服务提供者数据库的监控,具体的实现在 3.2 中给出。

3.2　基于 SPI 漏洞木马的查杀方法

针对基于 SPI 技术漏洞的新型木马,采用周期比较法实现的示例软件可以实现查杀功能。该软件共包括 3 个功能模块和一个系统服务提供者样本库,其中功能模块分别是提供者数据库监视模块、用户警示模块和木马清除模块,系统服务提供者样本库则保存了目前所有操作系统的标准服务提供者样本。周期比较法的程序流程简图如图 3 所示。

提供者数据库监视模块主要功能是定期扫描系统提供者数据库,然后在操作系统版本一致的情况下和系统服务提供者样本库的样本,比较若无差异则返回,继续定期扫描、对比;若不一致则调用用户警示模块。

警示用户模块主要功能是将监视模块传递来的异常情况,通过直观的图形界面显示给用户,并提醒用户系统的提供者数据库被修改,返回修改的相应参数,由用户判断允许或者拒绝,若选择允许则先备份修改的系统提供者数据库然后返回监视模块,否则调用木马清除模块。

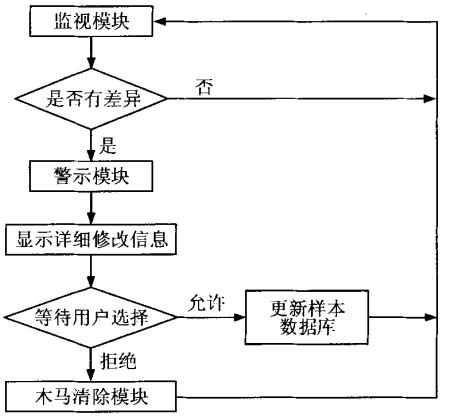

图 3　周期比较法的流程图

Fig. 3　The flow chart of periodic comparison method

木马清除模块主要功能则是调用 WSCDEInstall Provider( )函数清除安装的服务提供者,还原为最新备份的系统提供者数据库,然后返回监视模块。

4　结　论

本文详细分析了新木马的核心技术,并根据其实现的技术特性,提出了一套切实可行的木马查杀方法,为彻底清除木马提供了技术支持。本文虽然给出了对这类木马的防范思路和实现方法,但对该木马的判断还缺乏自动性和准确性,需要用户具备一定的安全知识,因此不太适合一般普通用户。下一步可以采用事件驱动代替定时查询的方法,提高防范的实时性、高效性,采用 DLL 跟踪技术,结合查杀 DLL 木马的技术实现对木马的自动化判定,更便于普通用户的使用。

参考文献:

[1]　施勇,薛质,李建华. 基于 SPI 及远程线程技术的新型木马研究[J]. 计算机工程,2005, 7(2):145-147.

[2]　JONES A. Windows 网络编程技术[M]. 北京:机械工业出版社,2000.

[3]　安娜,张凡,吴晓南,等. 一个基于移动 Agent 的分布式入侵检测系统[J]. 西北大学学报:自然科学版,2005, 35(1),25-28.

(编　辑　曹大刚)

A feasible defending method of a new Trojan horse based on service provider interface flaws

HE Xiao-wei[1], YU Jing-jing[2], WANG Miao[3]

(1. Information Science and Technology Institute, Northwest University, Xi'an 710069, China; 2. School of Physics and Information Technology, Shaanxi Normal University, Xi'an 710062, China; 3. School of Electronic & Information Engineering, Xi'an Jiaotong University, Xi'an 710049, China)

Abstract: Aim To keep away the new type of Trojan horse based on SPI. **Methods** Analyze the hiding mechanism of new Trojan proceeding from the principle of SPI technique and excogitate a method to check and clean this type of Trojan accordingly. **Results** A whole defending scheme was put forward for this new type Trojan horse and the implementation was described in detail. **Conclusion** At present, all kinds of existing anti-Virus applications can do nothing to the new type of Trojan horse based on SPI. A feasible periodic comparison method was provided to actualize automatic-manual cleaning of the new type Trojan horse.

Key words: service provider interface (SPI); new Trojan horse; anti-Trojan horse

(上接第906页)

Gait time series analysis for different physiological states using complexity-measure

TIAN Xu-zi[1], XU Jian-chun[2], HUANG Li-yu[2]

(1. Department of Computer Science, Baoji College of Arts and Science, Baoji 721007, China; 2. Department of Biomedical Engineering, Xidian University, Xi'an 710071, China)

Abstract: Aim To study gait, which in a certain sense, is a reflection of the health conditions and pathology of several diseases in human body. However, quantitative analysis of gait data has traditionally been a challenging task due to its multidimensionality, non-linear. The elaboration is dedicated to make a breakthrough in this field. **Methods** The definition and algorithm of LemZiv complexity were introduced, so the gait data analysis was implemented by using LemZiv complexity. **Results** The complexity is closely associated with age and other physiological status. **Conclusion** The effects of gait series length on complexity value were discussed to draw the conclusion that the complexity is model-independent and its calculation is rather simple, its application in the gait analysis is indeed promising.

Key words: gait; complexity-measure; Parkinson's disease

基于SPI技术漏洞的新型木马的防范方法

作者： 贺小伟， 余景景， 王淼， HE Xiao-wei， YU Jing-jing， WANG Miao

作者单位： 贺小伟,HE Xiao-wei(西北大学,信息科学与技术学院,陕西,西安,710069)， 余景景,YU Jing-jing(陕西师范大学,物理学与信息技术学院,陕西,西安,710062)， 王淼,WANG Miao(西安交通大学,电子与信息工程学院,陕西,西安,710049)

刊名： 西北大学学报（自然科学版） ISTIC PKU

英文刊名： JOURNAL OF NORTHWEST UNIVERSITY(NATURAL SCIENCE EDITION)

年，卷(期)： 2006,36(6)

参考文献(3条)

1. 施勇;薛质;李建华 基于SPI及远程线程技术的新型木马研究[期刊论文]-计算机工程 2005(02)

2. JONES A Windows网络编程技术 2000

3. 安娜;张凡;吴晓南 一个基于移动Agent的分布式入侵检测系统[期刊论文]-西北大学学报(自然科学版) 2005(01)

本文读者也读过(10条)