木马病毒分析及其检测方法研究

朱 明 徐 骞 刘春明
(中国科学技术大学自动化系,合肥 230027)
E-mail:mzhu@ustc.edu.cn

摘 要 特洛依木马作为一种新型的计算机网络病毒,它比其它病毒所构成对网络环境中计算机信息资源的危害都要大。文章对木马病毒特点和所采用技术方法进行了归纳研究,详细介绍了木马病毒在植入、加载、隐蔽、反清除、信息采集和网络通信等六方面所采用的技术方法;在此基础上,提出了基于多 Agent 协作实现未知新木马病毒自动识别新方法。该方法利用驻留在局域网各机器监测 Agent 和网络监测 Agent 所收集的证据和初步判断,并由协作 Agent 对这些证据和初步判断进行融合印证并做出最终结论。初步实验结果表明,该方法可以有效发现冰河木马病毒和广外女生木马病毒。

关键词 网络安全 木马病毒 病毒检测

文章编号 1002-8331-(2003)28-0176-04 **文献标识码** A **中图分类号** TP393.08

Analysis of Trojan Horse and Its Detection

Zhu Ming Xu Qian Liu Chunming
(Automation Department,The University of Science and Technology of China,Hefei 230027)

Abstract: Trojan horse ia a new kind computer virus,which makes much damage to computer information resoureces in a local network.This paper makes induction on charcteristics and techniques used in trojan horse virus,and introduces these technoques with respect to implanting,auto-loading,stealthy,anti-clearing,information gathering,communication in the trojan horse virus in detail.From there,a new approach based on multi-agent cooperative to realize trojan horse auto-detection is put forward.In this new method,monitor agents in each network computer and network make initial decision based on their evidence,then cooperative agent makes final decision based on the evidence from all monitor agents through data fusion.Initial experiment shows this method is able to detection IceRiver trojan horse and Broadcasting girl trojan hores.

Keywords: Network security,Trojan horse virus,Virus detection

1 前言

特洛伊木马(Trojan Horse,简称木马),是一种新型的计算机网络病毒程序。它利用自身所具有的植入功能,或依附其它具有传播能力病毒,或通过入侵后植入等多种途径,进驻目标机器,搜集其中各种敏感信息,并通过网络与外界通信,发回所搜集到的各种敏感信息,接受植入者指令,完成其它各种操作,如修改指定文件、格式化硬盘等。

目前木马常被用作网络系统入侵的重要工具和手段。感染了木马病毒的计算机将面临数据丢失和机密泄露的危险。除了针对个人用户,大型网络服务器也同样面临木马病毒的威胁,入侵者可通过对其所植入的木马而偷窃到系统管理员的口令。而当一个系统服务器安全性较高时,入侵者往往会通过首先攻破庞大系统用户群中安全性相对较弱的普通电脑用户;然后借助所植入木马获得这些普通用户的有效信息(如系统管理员口令),并最终达到侵入系统目标服务器的目的。最近的微软公司网络入侵事件就是这样一个典型的例子。

而在另一方面,木马病毒往往又被用做后门,植入被攻破的系统,以便为入侵者再次访问(被攻破的)系统提供方便;或者利用被入侵的系统,通过欺骗合法用户的某种方式暗中散发木马病毒,以便进一步扩大入侵成果和入侵范围,为进行其它入侵活动,如分布 DoS 攻击提供可能。

作为一种新型的网络病毒,木马与普通病毒相比,包括其它网络病毒,如蠕虫病毒,仍存在着很大差异,这种差异主要体现在木马病毒设计所涉及有关技术与功能这两方面。一般病毒的设计主要侧重于其隐蔽性和传播性的实现;而木马病毒除此之外,还更多地强调与外界通信,以及反清除与反识别能力。不能正确清楚地了解木马病毒与一般病毒的主要区别,无疑将会给木马病毒的有效防范造成消极的影响。现在有很多防病毒软件都将木马病毒视为一类简单病毒,仍采用传统的反病毒技术来检测和清除木马。这样做很难彻底清除(所发现的)木马病毒。以下将会看到利用现有反病毒技术,很难发现和清除一个精心设计的木马病毒。防治木马必须要有新的思路。

该文第二节介绍当前木马病毒特点及其设计所采用的最新技术手段,第三节介绍一种可以有效检测木马病毒,尤其是能够有效检测新奇未知木马病毒的多 Agent 分布协作检测方法;最后一节则是关于木马病毒检测技术与方法的总结。

2 木马病毒分析

一个典型的特洛伊木马(程序)通常具有以下四个特点:有效性、隐蔽性、顽固性和易植入性。一个木马病毒的危害大小和

作者简介:朱明(1963-),男,副教授,主要研究方向:网络安全、数据挖掘等。

清除难易程度可以从这四个方面来加以评估。它们是：

(1)有效性：由于木马病毒常常构成网络入侵方法中的一个重要内容。它运行在目标机器上就必须能够实现入侵者的某些企图，因此有效性就是指入侵的木马能够与其控制端(入侵者)建立某种有效联系，从而能够充分控制目标机器并窃取其中的敏感信息。因此有效性是木马病毒的一个最重要特点。入侵木马对目标机器的监控和信息采集能力也是衡量其有效性的一个重要内容。

(2)隐蔽性：木马病毒必须有能力长期潜伏于目标机器中而不被发现。一个隐蔽性差的木马往往会很容易暴露自己，进而被杀毒(或杀马)软件，甚至用户手工检查出来，这样将使得这类木马变得毫无价值。因此可以说隐蔽性是木马病毒的生命。

(3)顽固性：当木马病毒被检查出来(失去隐蔽性)之后，为继续确保其入侵有效性，木马病毒往往还具有另一个重要特性：顽固性。木马病毒顽固性就是指有效清除木马病毒的难易程度。若一个木马在检查出来之后，仍然无法将其一次性有效清除，那么该木马病毒就具有较强的顽固性。

(4)易植入性：显然任何木马病毒必须首先能够进入目标机器(植入操作)，因此易植入性就成为木马病毒有效性的先决条件。欺骗性是自木马病毒诞生起最常见的植入手段。因此各种好用的小功能软件就成为木马病毒常用的栖息地。利用系统漏洞进行木马植入也是木马病毒入侵的一类重要途径。目前木马技术与蠕虫技术的结合使得木马病毒具有类似蠕虫的传播性，这也就极大提高了木马病毒的易植入性。

近年来，木马病毒技术取得了较大的发展，目前已彻底摆脱了传统模式下植入方法原始、通信方式单一、隐蔽性差等不足。借助一些新技术，木马病毒不再依赖于对用户进行简单的欺骗，也可以不必修改系统注册表，不开新端口，不在磁盘上保留新文件，甚至可以没有独立的进程，这些新特点使对木马病毒的查杀变得愈加困难；但与此同时却使得木马的功能得到了大幅提升。采用了新技术的木马病毒可以轻易穿过防火墙与外界(入侵者)通信。

以下将分别对木马病毒的植入技术、加载技术、反清除技术、隐藏技术、信息获取技术和通信技术作进一步的介绍，从而可以对木马病毒实质能够有一个更全面清晰的认识。

2.1 木马病毒的植入技术

木马病毒植入技术，主要是指木马病毒利用各种途径进入目标机器的具体实现方法。目前常用的木马植入技术主要分为三类：伪装欺骗、利用系统漏洞和入侵后直接植入。此外利用蠕虫传播技术进行木马病毒正在成为木马病毒植入技术的一个重要发展趋势。以下就对前两类植入方法作一简要介绍：

2.1.1 伪装欺骗

通过更改木马病毒程序(文件)的文件后缀和图标等，将其伪装成一个有用的程序、文本文件或多媒体文件，然后藏匿在电子邮件的附件中，并在目标机器用户受骗点击相应藏有木马程序的文件图标时自动完成木马病毒的植入操作，这是目前大多数木马病毒所采用的植入方法。

例如：利用 Windows 操作系统对特定文件扩展名采取隐蔽的做法，即使在系统中设置显示已知类型文件的扩展名选项，某些特殊类型的文件扩展名仍然不能被显示。这样的文件类型包括“碎片对象文件(*.shs)”和“快捷方式连接文件(*.lnk)”等。因此一个名为 danger.txt.shs 的文件在此系统中将显示为 danger.txt。显然这一不足可以被利用作为木马植入途径。另一种伪装欺骗就是将木马程序同其它软件捆绑在一起以实现欺骗式植入。当用户运行执行捆绑有木马病毒的应用程序时，木马病毒就得以植入；这时由于原来的应用程序仍可正确执行，从而使得用户无法察觉到木马病毒的植入行为。更有甚者目前已有可将木马程序拆开存放在其宿主程序文件的空隙处，从而使捆绑木马病毒的程序文件大小不发生变化的捆绑工具。

2.1.2 利用系统漏洞

由于各种操作系统、应用软件系统在最初编制完成时，会遗留各种软件编程不足，如各种缓冲区溢出漏洞，这些不足很容易被利用以实现木马病毒的植入。

例如：可将一个木马病毒伪装成一个图像文件并在一个 Web 网页中引用，则当目标机用户浏览此 Web 页时(打开超文本电子邮件也同样)，浏览器就会自动下载此文件并存放于 Internet 历史记录文件夹中；之后只要通过网页中的脚本程序查找到该“图像”文件并对其复原，就可以有效完成木马病毒的植入。

由于操作系统软件规模的庞大，其内部不可避免地存在各种缺陷。有些缺陷构成了系统安全上的漏洞。虽然漏洞可以用补丁进行修补，但新的漏洞还会不断被发现。如最新两个典型的 Windows 系统漏洞，利用这两种漏洞自然成为目前最为有效的木马植入方式。

(1)IIS UNICODE 解码漏洞

该漏洞于 2000 年 10 月 17 日公布并被微软公司的正式命名为“Web Server Folder Traversal 漏洞”。Windows NT 4.0 上的 IIS4.0 和 Windows2000 上的 IIS5.0 都存在该漏洞。据不完全统计，从 2000 年 10 月开始，黑客入侵 Windows 系统所采取的方法中有近 70%是通过这个漏洞进行的。

该漏洞就是：当 IIS 服务器中的一个文件被打开时，若该文件名包含有 UNICODE 字符的话，系统会对其进行解码。而某些特殊的 UNICODE 码会导致服务器错误的打开或执行超过其网站所限定目录以外的文件，这就会为入侵者植入木马病毒提供可能的机会。类似的漏洞还有 IIS 4.0 ISM.DLL 缓冲区溢出漏洞和 MDAC/RDS 漏洞等等。

(2)IE 处理 MIME 漏洞

这是 IE 在处理 MIME 邮件时的一个漏洞。也就是：当一个可执行文件经过 base64 编码后定义为声音类型并作为 MIME 文件打开时，系统会将其中可执行文件误认为是背景声音而在加载时使其直接获得运行。利用此漏洞进行木马植入也是目前一种常用且相当有效的方法。

显然随着各种系统漏洞的不断发掘，木马病毒的植入技术也必将随之不断地推陈出新。

2.2 木马病毒的加载技术

当木马病毒成功植入目标机后，就必须确保自己可以通过某种方式得到自动运行。常见的木马病毒加载技术主要包括：系统启动自动加载、文件关联和文劫持等。下面对这些技术作一简要介绍：

2.2.1 系统启动自动加载

这是最常用的木马自动加载方法。木马病毒通过将自己拷贝到启动组，或在 win.ini、system.ini 或注册表中添加相应的启动信息而实现系统启动时自动加载。这种加载方式简单有效，但隐蔽性差。目前很多反木马软件都会扫描注册表的启动键(信息)。故而新一代木马病毒都采用了更加隐蔽的加载方式。

2.2.2 文件关联

这是通过修改注册表来完成木马的加载。但它并不直接修

改注册表中的启动键(信息),而将其与特定的文件类型相关联,如与文本文件或图像文件相关联。这样在用户打开这种类型的文件时,木马病毒就会被自动加载。

2.2.3 文件劫持

文件劫持是一种特殊的木马加载方式,为此木马病毒被植入到目标机后,需要首先对某个系统文件进行替换或嵌入操作,使得该系统文件在获得访问权之前,木马病毒被率先执行,然后再将控制权交还给相应的系统文件。采用这种方式加载木马不需要修改注册表,从而可以有效躲过注册表扫描型反木马软件的查杀。

这种方式最简单的实现方法是将某系统文件改名,然后将木马程序改名。这样当这个系统文件被调用的时候,实际上是木马程序被运行,而木马启动后,再调用相应的系统文件并传递原参数。

2.3 木马病毒的反清除技术

为确保有效性,木马病毒常常具有一定反清除能力。主要反清除技术包括:多实例、系统内核嵌入和 BIOS 写入等。下面对这些技术作一简要介绍。

2.3.1 多实例

所谓多实例就是将木马程序(多份)分别存放在目标机的不同目录下,这些木马实例彼此相互监督,以防止某个木马病毒实例被查杀。冰河木马就采用了双份独立存放方法。一份与文本文件相关联,因此当一份被删除后,另一份会在打开文本文件时,重新生成被删除的那份木马程序。

此外有些木马病毒还采用同时运行多个进程(或线程),彼此采用信号量或触发事件来实现互相监视,当一个进程(或线程)被杀死时,其它进程(或线程)就会立刻重新生成该进程(或线程)的实例。

显然采用多实例的木马具有较强的顽固性。现在许多木马病毒就采用了这样的技术。

2.3.2 操作系统内核嵌入

木马病毒如果已获取了操作系统的部分控制权,就可以将自己紧密地依附到系统部件上,这就使木马查杀变得更加困难。后面将要介绍的利用设备驱动技术就是其中一种。

2.3.3 BIOS 写入

BIOS 是系统的基本输入输出系统,存放于 EEPROM 芯片上。如果将特定的木马代码写入 BIOS,将会使木马更加难于清除。借助 BIOS 会大大提高木马病毒的顽固性。

2.4 木马病毒的隐藏技术

为确保有效性,木马病毒必须具有较好的隐蔽性。木马病毒的主要隐蔽技术包括:伪装、进程隐藏、DLL 技术等。

2.4.1 伪装

从某种意义上讲,伪装是一种很好的隐藏。木马病毒的伪装主要有文件伪装和进程伪装。前者除了将文件属性改为隐藏之外,大多通过采用一些比较类似于系统文件的文件名来隐蔽自己;而后者则是利用用户对系统了解的不足,将自己(木马)进程名设为与系统进程类似而达到隐藏自己的目的。

2.4.2 进程隐藏

木马病毒进程是它驻留在系统中的最好证据,若能够有效隐藏自己的进程,显然将大大提高木马病毒的隐蔽性。在 Windows98 系统中可以通过将自己设为系统进程来达到隐藏进程的目的。但这种方法在 Windows NT/2000 下就不再有效,只能通过下面介绍的 DLL 技术或设备驱动技术来实现木马病毒的隐藏。

2.4.3 DLL 技术

采用 DLL 技术实现木马的隐蔽性,主要通过以下两种途径:DLL 陷阱和 DLL 注入。

(1)DLL 陷阱

DLL 陷阱技术是一种针对 DLL(动态链接库)的高级编程技术,通过用一个精心设计的 DLL 替换已知的系统 DLL 或嵌入其内部,并对所有的函数调用进行过滤转发。对于正常的调用直接转发给被替换的系统 DLL;而对于特定情况,则首先会执行一些木马操作。采用这种技术的木马没有明显独立程序文件,也不开单独的进程,因而具有较好的隐蔽性。

(2)DLL 注入

DLL 注入技术是将一个 DLL 注入到某个进程的地址空间,然后潜伏在其中并完成木马的必需操作。DLL 注入的方法有很多种,比较有效的是修改注册表和远程线程技术(Remote Thread)。所谓远程线程技术就是通过在另一个进程中创建远程线程的方法进入该进程的地址空间。被创建的远程线程可以共享远程进程的地址空间。在远程嵌入完成,再将原进程关掉,这样系统中就不留有任何痕迹了。

2.4.4 设备驱动技术

从广义上讲,设备驱动程序就是控制硬件设备的一组函数。在 Windows 系统中下共有三种设备驱动:VxD、KMD 和 WDM。VxD(Virtual Device Driver)起源于 Windows 3.1 时代,现在仍然应用在 Windows 95/98/ME 中。它运行于系统保护层(Ring 0),可以完成各种系统物理层访问。KMD(Kernel Mode Driver)是一个在 Windows NT 下提出的管理、维护硬件运作的驱动程序模式。WDM(Win32 Driver Model)是微软公司力推的全新驱动程序模式。虽然它效率较低,实现比较复杂,但在 Windows2000 下,它是唯一支持的模式。

利用设备驱动的木马显然具有很好的顽固性和隐蔽性。如何防范这种木马,是一个值得认真思考的问题。

2.5 木马病毒的信息获取技术

获取目标机的各种敏感信息,是木马病毒有别于其它病毒或蠕虫的最大特点之一。木马病毒原则可以获取目标机中所有信息,这其中包括:(1)基本信息,如系统版本、用户名、系统目录等;(2)利用钩子函数获取用户键入的口令或其它输入;(3)对目标机所在局域网中流动的信息包进行嗅探,以获得诸如系统口令或其它敏感信息;(4)目标机屏幕截取与传送;(5)目标机附近声音信号的采集与传输。

2.6 木马病毒的通信技术

与主控机进行通信,以接受主控机指令并发送所窃取的各种重要信息,是木马病毒有别于其它病毒或蠕虫的最大特点。驻留到目标机的木马病毒与主控机进行通信的方式有:

(1)传统的客户/服务通信模式:即木马病毒打开某个端口进行监听以获得主控机的连接消息,以便与之进行通信交流;

(2)端口寄生,就是木马病毒利用目标机上一个已经打开的端口进行监听(寄生之上),遇到(来自主控机的特殊格式)指令就进行解释执行;由于这时木马实际上是寄生在(目标机)已有的系统服务之上,因此无法通过系统端口扫描发现此类木马病毒;

(3)端口反弹,由于绝大多数防火墙都严格限制由外向内的连接请求,故工作在传统客户/服务通信模式下的木马往往很难奏效。而端口反弹型木马则恰恰相反,它利用了防火墙对

由内向外的连接请求通常不加限制的特点，将主控机作为服务器，而目标机作为客户，主动向外发出连接请求。如将主控机监听端口设为80，伪装成Web服务器，则目标机的通信请求都会被防火墙误认为是HTTP请求而予以通行；

(4)利用应用层协议，木马为了避开新端口以增加其隐蔽性，往往会利用现有的高层协议，如HTTP协议、FTP协议或SMTP协议(与主控机)进行通信交流。为此木马主控机会伪装成一个支持CGI的HTTP服务器，在80端口监听(来自目标机的)连接请求。而目标机则可以利用HTTP协议与主控机进行通信交流，传送目标机中的重要敏感信息；

(5)利用ICMP协议，木马病毒利用ICMP协议进行通信交流，可以有效避免被端口扫描工具所察觉，以增强其隐蔽性。但是由于ICMP协议不是一个可靠的有连接传输，因此只能用来传递一些敏感信息，而不适合用来进行实时图像传输和远程控制。同时由于目前基于ICMP的攻击方式很多，有些防火墙阻塞了ICMP包，在这种情况下，利用ICMP协议的木马病毒就失灵了；

(6)对网卡或Modem直接编程，为防止通过检测WinSock调用来发现自己，木马病毒在与外界通信时就不能利用套接字，这样唯一的办法就需要直接针对网卡或Modem进行编程。鉴于篇幅和安全原因，这里将不再对上述技术方法作进一步的介绍。

3 木马病毒检测方法

由于木马病毒在其植入、加载、反清除、隐蔽、信息获取和通信交流这六个方面，所采用的方法五花八门，仅目前公开的各种木马技术方法就有近百种，显然随着计算机软件系统不断发展各种木马病毒技术方法无疑也将会不断出新。

尽管国内外都推出了一些杀马软件，如：Anti-Trojan 5.5，就号称目前可以查杀8000余种已知木马病毒。但如何有效发现新奇(未知)木马病毒，目前尚未提出什么较好方法，针对这一情况，该文提出一种可以有效发现新奇(未知)木马病毒的方法，该方法可以在局域网环境中，自动发现新出现的木马病毒。该方法利用木马病毒在植入、加载、反清除、隐蔽、信息获取和通信交流这六个方面所要达到目标和所采用方法的本质，实现对木马病毒的自动识别。这里所提出的方法与目前普遍采用病毒特征库的方法明显不同，正因为如此，该方法可以发现未知的新木马病毒。

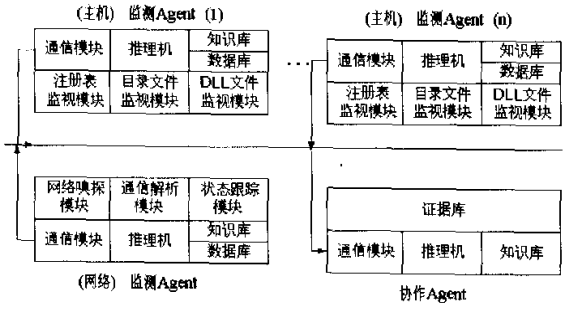

图1 基于多Agent协作的新奇木马自动识别系统框架

文章所提方法是一种基于多Agent协作机制实现新奇木马病毒自动检测的新方法，该方法的基本系统框架如图1所示。这里将主要介绍图1所示新方法的应用环境及其木马病毒识别基本思想等主要内容，具体内容介绍如下：

(1)新方法主要用于对局域网中多台机器中可能存在的木马病毒进行自动识别。该方法可以实现对局域网中具有自主传播能力的木马病毒(如：蠕虫类木马病毒)进行(不依赖木马病毒特征库)的主动识别；

(2)新方法目前主要是根据木马病毒三个重要特点：①它必须与外界主控机进行通信交流，接受指令并发送所窃取到的重要信息；②它会读取用户关键资料，如密码口令或其它敏感信息文件等；③它会千方百计将自己隐藏到系统文件(如：注册表、DLL文件，甚至是设备驱动等)中，来实现对木马病毒，尤其对新出现木马病毒的自动识别；

(3)新方法采用了基于(将划分与层次聚类相结合的)异类挖掘方法，对局域网中的中马机器及其网络监听所获得的(事件、活动)数据记录进行分析处理；在此基础上，利用所形成的多Agent(局域网中每台机器均驻留一个Agent)环境，根据“同一木马病毒在各感染机器上表现均应基本相同”这一假设，利用由多个Agent所发现的多个证据进行相互印证，以最终实现对(未知)新奇木马病毒的发现与识别。

在该文所提方法中，局域网中的每台机器均驻留一个主机监测Agent，以负责对相应机器中注册表内容变动和系统目录下文件(数目和内容)变动情况进行非实时的监视；同时还将设置一台独立机器，其上驻留一个网络监测Agent和一个协作Agent，其中网络监测Agent专门负责对局域网中各机器网络通信情况进行监测；而该机上的协作Agent则负责接受来自各主机监测Agent的个体决策和相关证据，然后利用数据融合方法对来自各机个体决策和相关证据进行印证融合，并给出局域网各机器中是否存在木马病毒的最终结论。

目前应用该方法所完成的初步实验，在不依赖病毒特征库情况下，可以发现冰河木马病毒和广外女生木马病毒。

4 工作总结

由于木马病毒技术涉及系统基础内容较多，且发展迅速。充分深入地研究木马病毒技术对防范木马病毒，提高网络系统的安全性具有重要的意义。

通过对木马病毒技术方法的研究归纳，可以清楚地发现，木马病毒，同其它计算机病毒一样，都处在不断的发展和进化的当中。传统的木马病毒在反木马软件、端口扫描软件和防火墙的围攻之下，不仅没有消失，反而很快就以更新、更强、更高级的形式(新一代木马病毒)又出现了。

文章所提出的基于多Agent协作实现对未知新木马病毒的自动检测方法，仅仅是在尝试从更高层次实现对木马病毒自动检测方面迈出的第一步。随着采用新技术、利用系统新漏洞木马病毒的不断出现，反木马病毒理论和技术必将同时也必需不断发展。(收稿日期：2003年1月)

参考文献

1.Secrets and Lies.Digital Security in a Networked World[M].Bruce Schneier:John Wiley & Sons,Inc,2001

2.鲍友仲.飞思科技产品研发中心.网络安全之防黑秘诀[M].电子工业出版社,2002

3.卢勇焕，郑海允，崔吉俊(韩).黑客与安全[M].中国青年出版社,2001

4.http://www.yesky.com/

木马病毒分析及其检测方法研究

作者： 朱明， 徐骞， 刘春明
作者单位： 中国科学技术大学自动化系,合肥,230027
刊名： 计算机工程与应用 ISTIC PKU
英文刊名： COMPUTER ENGINEERING AND APPLICATIONS
年，卷(期)： 2003,39(28)
被引用次数： 36次

参考文献(4条)

1. Secrets Digital Security in a Networked World 2001
2. 鲍友仲 飞思科技产品研发中心网络安全之防黑秘诀 2002
3. 卢勇焕;郑海允;崔吉俊 黑客与安全 2001
4. 查看详情

本文读者也读过(6条)

1. 宋海涛 木马攻击防范理论与技术研究[学位论文]2004
2. 张新宇.卿斯汉.马恒太.张楠.孙淑华.蒋建春 特洛伊木马隐藏技术研究[期刊论文]-通信学报2004,25(7)
3. 杨彦.黄皓.YANG Yan.HUANG Hao 基于攻击树的木马检测方法[期刊论文]-计算机工程与设计2008,29(11)
4. 李焕洲.唐彰国.钟明全.张健.LI Huan-zhou.TANG Zhang-guo.ZHONG Ming-quan.ZHANG Jian 基于行为监控的木马检测系统研究及实现[期刊论文]-四川师范大学学报（自然科学版）2009,32(3)
5. 何鸿君.罗莉.董黎明.何修雄.候方勇.钟广军.HE Hong-Jun.LUO Li.DONG Li-Ming.HE Xiu-Xiong.HOU Fang-Yong.ZHONG Guang-Jun 广义病毒的形式化定义及识别算法[期刊论文]-计算机学报2010,33(3)
6. 康治平.向宏.Kang Zhiping.Xiang Hong 特洛伊木马隐藏技术研究及实践[期刊论文]-计算机工程与应用2006,42(9)

引证文献(37条)

1. 崔宝才 SysAnti.exe病毒的分析与防范[期刊论文]-信息系统工程 2012(6)
2. 张洪进 木马隐藏技术初探[期刊论文]-医疗卫生装备 2011(4)
3. 郑枫 关于特洛伊木马攻击的探析[期刊论文]-数字技术与应用 2011(3)
4. 张春诚.路刚.冯元 木马通信的隐蔽技术[期刊论文]-电脑知识与技术 2008(35)
5. 康乐.韩俊杰.刘胜利 利用进程监视来检测Http-Tunnel[期刊论文]-计算机工程与应用 2006(7)
6. 戴敏.黄亚楼.王维 基于文件静态信息的木马检测模型[期刊论文]-计算机工程 2006(6)
7. LI Zhi-yong.ZHANG Hao.TAO Ran.DU Hua A Vicious Script in HTML Detection Method Using Judgment Matrix Approach[期刊论文]-兵工学报（英文版） 2009(1)
8. 张昊.陶然.李志勇.杜华 判断矩阵法在网页恶意脚本检测中的应用[期刊论文]-兵工学报 2008(4)
9. 曹光辉.鄂旭.杜颖.马雨时 一种全新的木马自启动方案[期刊论文]-渤海大学学报（自然科学版） 2008(4)
10. 姜坚.袁家斌 基于特征行为的远程访问型木马阻断技术[期刊论文]-计算机与数字工程 2008(11)
11. 陈熔 木马病毒分析及其防治方法[期刊论文]-农业网络信息 2006(5)
12. 唐毅 木马攻击方式的分析与应对[期刊论文]-计算机光盘软件与应用 2010(10)
13. 陶阳 一种双链路的特洛伊木马设计与实现[期刊论文]-电脑编程技巧与维护 2009(22)
14. 侯明明 浅析"木马"病毒及其防治措施[期刊论文]-广西轻工业 2009(3)
15. 蔡洪民.伍乃骐.滕少华 特洛伊木马攻击分析与检测技术研究[期刊论文]-计算机安全 2007(4)

16. 凌循 木马病毒的分析与防治[期刊论文]-电脑知识与技术(学术交流) 2007(7)

17. 孙锋 木马病毒的分析与防治[期刊论文]-科技资讯 2006(28)

18. 贾学东. 陈喆. 张晓艳. 孟健 新型网络蠕虫特征分析及防御策略[期刊论文]-信息工程大学学报 2004(3)

19. 王泽东. 刘宇. 朱随江. 刘宝旭. 潘林 采用行为分析的单机木马防护系统设计与实现[期刊论文]-计算机工程与应用 2011(11)

20. 陆军 浅谈木马的防御与查杀[期刊论文]-科技致富向导 2011(9)

21. 周鹏 计算机病毒的防治策略[期刊论文]-牡丹江师范学院学报（自然科学版） 2010(1)

22. 王立新. 武鼎 通过特洛伊木马认识木马[期刊论文]-科技资讯 2008(12)

23. 李志勇. 陶然. 王越. 张昊 溢出型网页恶意代码运行机理分析与防范[期刊论文]-兵工学报 2010(6)

24. 袁娣 基于木马控制的网络监控系统设计[期刊论文]-船海工程 2009(2)

25. 罗红. 慕德俊. 戴冠中. 袁源 端口反弹型木马的通信技术研究[期刊论文]-微电子学与计算机 2006(2)

26. 钱昌明. 黄皓 Linux木马检测技术分析与系统调用权限验证法[期刊论文]-微型机与应用 2005(6)

27. 陈俊周 基于水印的隐蔽入侵及防范[学位论文]硕士 2004

28. 郝东白. 郭林. 黄皓 基于限定令牌的木马防护系统设计[期刊论文]-计算机工程与应用 2007(24)

29. 庄小妹 木马的入侵检测技术和清除方法[期刊论文]-内江科技 2006(7)

30. 李志勇. 薛亮. 陶然. 张昊 跨安全域网页恶意代码运行机理与防范[期刊论文]-计算机工程与应用 2010(21)

31. 韩芳. 栾国森 远程线程注入木马的攻防研究[期刊论文]-计算机与数字工程 2008(3)

32. 张亮. 陈雷霆 基于人工免疫机制的木马检测子系统[期刊论文]-计算机科学 2004(10)

33. 唐树刚 基于文件静态特征的木马检测研究[学位论文]硕士 2005

34. 陈京浩 进程检测模型及相关技术的研究与实现[学位论文]硕士 2005

35. 于志刚. 蒋璟 关于"木马"侵入行为的刑法学思索[期刊论文]-中国人民公安大学学报（社会科学版） 2008(6)

36. 潘洪涛 计算机免疫中“非我”分类的研究[学位论文]硕士 2005

37. 岳新 Linux2.4内核下基于Netfilter框架可扩展性研究与实现[学位论文]硕士 2005