特种木马

防御与检测技术研究

孙建国 / 主编
赖明珠 高 迪 姜 莉 田秀霞 / 编著

中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

特种木马

防御与检测技术研究

孙建国 / 主编
赖明珠 高 迪 姜 莉 田秀霞 / 编著

人民邮电出版社
北京

图书在版编目（CIP）数据

特种木马防御与检测技术研究 / 孙建国主编 ; 赖明珠等编著. -- 北京 : 人民邮电出版社, 2015.12
ISBN 978-7-115-39609-9

Ⅰ. ①特… Ⅱ. ①孙… ②赖… Ⅲ. ①计算机网络－安全技术 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2015)第137353号

内 容 提 要

本书以作者近几年在信息安全领域的研究经历为基础，系统介绍了木马检测与防护的关键技术。内容涵盖木马行为的基本理论、木马基本特征、木马检测与防护各阶段的关键技术。

本书内容简练，通俗易懂。既可供高等院校信息安全，特别是信息系统安全相关领域的师生使用，又可以作为开发人员和技术人员的设计参考书，也可供对系统安全、木马防护技术感兴趣的读者阅读。

◆ 主　　编　孙建国
编　　著　赖明珠　高　迪　姜　莉　田秀霞
责任编辑　邢建春
执行编辑　吴彤云
责任印制　彭志环
◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京隆昌伟业印刷有限公司印刷
◆ 开本：880×1230　1/32
印张：6.5　　2015 年 12 月第 1 版
字数：210 千字　　2015 年 12 月北京第 1 次印刷

定价：49.00 元

读者服务热线：（010）81055488　印装质量热线：（010）81055316
反盗版热线：（010）81055315

前 言

2011 年以来，面向我国信息网络的网站入侵、网络欺诈等恶意网络行为依然呈现上升趋势，特别是移动领域的恶意行为大幅增加。微软、谷歌、思科、苹果、雅虎等科技公司的产品已深入国内各部门、企事业单位，并培养了数以亿计的忠实用户，用户在使用过程中信息很容易被监听、过滤，这使我国的信息安全几乎毫无保障可言。

“棱镜”事件再次凸显了我国信息系统安全的整体态势，同时，也暴露出现有的信息安全等级测评以及管理制度的真空。倘若斯诺登所言非虚，不知又将置“我们多年的信息安全等级测评工作以及网络安全防范体系”于何地？因此，“棱镜”事件必然为我国现有的信息安全管理体系敲响警钟，“合理完备、客观周密”的信息流动与管控立法将为期不远。

《管子》中有句话叫“墙有耳，伏寇在侧”。针对涉密信息管控领域，为防止涉及国家秘密的计算机及信息系统受到来自互联网等公共信息网络的攻击，确保国家秘密信息的安全，党和国家多次强调要求涉密计算机及信息系统要与互联网等公共信息网实行物理隔离。从单纯的技术防御体系来看，物理隔离技术解决了数据边界的安全问题，将外部环境与内部涉密信息隔绝开，且必需的数据交换均处于管控范围之内。但实质上，物理隔离的设计者和建设者往往忽略了信息流动的必然和多源特点，面对信息的产生、加工、处理、存储以及传播、销毁等全生命周期，依靠单纯的物理隔离是无法完全实现的，必须对信息流动的管理进行加固。

面对如此紧迫的网络安全问题和涉密信息系统安全瓶颈，我们的信息安全研究团队开展了积极的研究工作。在确定研究方向的时候，主要考虑以下3个问题：1）必须是一个关系信息系统安全运行的关键命题；2）必须是一个实际的科研问题，不那么虚无缥缈；3）必须是一个交叉领域问题，不需要过于热门。在这样的背景下，结合社会需求和知识积累，产生了科研方向为木马防御与检测技术的研究。

2008年9月，团队正式开始进入特种木马的研究阶段，当时能够检索到的国内外核心期刊论文和会议论文不过百篇，这对于一个研究方向或者领域来说，数目可谓寥寥无几。但是，我坚信这个领域不会太冷，而且一定会逐渐“春暖花开”。事实证明，当时的想法是对的。当然这是后话，在当时我理清了思绪，耐心阅读了所有可检索到的论文，并进行了适当扩展性阅读。值得一提的是，在此阶段，项目组完成了军工领域特种木马防御与检测技术研究报告。

完成基础研究报告后发现：特种木马的种类繁多，所依托的理论、模型千差万别，如何进行比较和性能分析？不知彼长，如何确定己短？衡量的标准是什么，指标体系如何确定？为此，决定从性能评测入手，分为恶意代码、特种木马和常规病毒3类进行展开；同时，在此研究阶段，项目组进一步细分，逐渐形成了系统环境检测、进程系统、文件系统、注册表系统、恶意代码以及网络系统6个研究小组。

我们的研究思想是:以涉密信息系统为研究对象，以保障信息系统内数据安全为研究内容，从木马攻击以及检测防护的实用角度出发，深入研究可满足涉密信息系统内数据安全可控、广泛应用的信息安全技术。首先，结合信息系统的实际特点，分析和阐述病毒、木马的基本原理，并提出基本的木马防范与检测措施。在此基础上，提出整体研究框架和数据库设计方案，说明检测与清除的基本流程。其次，从注册表、文件系统、网络系统和进程系统4个方面，利用驱动过滤技术提出实现和设计思路。同时，基于动态检测与静态匹配相结合的思路，提出不同类型木马特征库的设计与实现思路。最

后，本书对摆渡木马进行了重点检测，特别是U盘、光盘等摆渡攻击的实现原理进行了介绍。

从特种木马的静态特征和行为特征出发，比较全面、系统地论述了木马检测与清除的关键理论和技术问题，主要内容包括木马的基本特征、木马攻击的基本原理、静态木马检测技术、动态行为分析与匹配技术、特征木马清除技术等。

全书共8章，每章都包含了作者近年的科研成果。第1章简要介绍病毒、木马的基本原理与本质特征。第2章提出木马检测与防护系统的整体框架。从木马静态与动态行为特征的研究入手，介绍了针对信息系统的各种攻击方式及防护技术，最后重点介绍了基于静态特征的木马检测方法。第3章针对木马行为特征的主要过程，提出了木马检测与清除的关键性技术，即逻辑过程分析、文件系统扫描与清除、文件隔离与清除、恶意文档检测与清除。第4章针对木马渗透攻击的主要环节，提出了木马防护的主要手段，利用消息拦截与驱动过滤方法，提出了动态防御的整体策略，包括注册表驱动过滤、文件系统驱动过滤、网络协议驱动过滤以及进程驱动过滤。第5章基于第3章和第4章的研究成果，重点研究了木马特征库的设计与加载方式，融入了木马静态特征、动态行为特征以及自定义的关键特征的识别问题。第6章介绍特种木马防护模块设计。第7章说明特种木马特征库设计。第8章是系统演示和总结部分。在本书的最后，作者着重介绍了当前比较流行的特征木马的行为特征，以及主要的防护与检测手段，李佳楠同学对光盘刻录以及移动存储硬盘的特种木马与防护给出了详细的描述。

本书是哈尔滨工程大学信息安全研究团队全体师生的研究成果结晶。本书是国家自然科学基金、教育部高等学校博士点基金、黑龙江省政府博士后资助项目、国家军工保密资格审查认证中心合作项目的成果总结。在写作过程中，博士生寇亮，硕士生苗施亮、谭凯、于成、胡俊夫、李春晓等，本科生李佳楠、李博权等都付出了辛苦工作。特别感谢哈尔滨工程大学张国印教授、印桂生教授、武俊鹏教授、高迪老师的帮助，以及对本书及相关研究工作的支持和鼓励。

希望本书能为推进我国信息系统数据安全的研究尽绵薄之力。限于作者水平，书中定有疏漏和不当之处，希望大家批评指正和交流，欢迎通过电子邮件（sunjianguo@hrbeu.edu.cn）联系。

目 录

第 1 章 绪论 …… 1

1.1 背景及意义 …… 1
1.2 木马的检测与防护 …… 3
1.2.1 特种木马的基本特征 …… 4
1.2.2 特种木马隐藏技术 …… 5
1.2.3 特种木马的免杀 …… 8
1.2.4 木马检测与防护的技术要求 …… 9
1.2.5 特种木马的关键行为特征 …… 10
1.3 国内外研究情况 …… 12
1.3.1 摆渡木马植入技术研究（1990~2001 年） …… 12
1.3.2 摆渡木马隐藏技术研究（2005~2010 年） …… 13
1.3.3 摆渡木马分析技术研究（2011 年至今） …… 14
1.4 主流木马检测技术 …… 15
1.4.1 特征码检测技术 …… 15
1.4.2 基于文件静态特征的检测技术 …… 17
1.4.3 文件完整性检测技术 …… 19
1.4.4 虚拟机检测技术 …… 21
1.4.5 行为分析技术 …… 22
1.4.6 入侵检测技术 …… 23
1.4.7 云安全技术 …… 26
1.5 本章小结 …… 27

第 2 章　特种木马技术的基本原理 …… 28

2.1　U 盘摆渡木马特征分析 …… 28
2.1.1　摆渡执行过程 …… 29
2.1.2　文件搜索 …… 34
2.1.3　写入 U 盘等移动介质 …… 34
2.1.4　发送被窃取文件 …… 36
2.1.5　启动方式的隐藏 …… 36
2.2　DLL 型摆渡木马的设计原理 …… 39
2.2.1　DLL 基础知识 …… 39
2.2.2　整体设计框架 …… 42
2.3　DLL 木马生命周期简介 …… 43
2.3.1　木马注入 …… 44
2.3.2　劫持系统 DLL …… 45
2.3.3　木马隐藏 …… 47
2.3.4　DLL 木马免杀策略 …… 54
2.3.5　DLL 木马自毁策略 …… 58
2.4　仿真实验分析 …… 59
2.4.1　环境介绍 …… 60
2.4.2　流程介绍与分析 …… 61
2.4.3　实验结果分析 …… 65
2.5　本章小结 …… 66

第 3 章　PE 类型木马技术原理 …… 67

3.1　PE 文件结构 …… 67
3.1.1　DOS MZ Header …… 68
3.1.2　PE Header …… 68
3.1.3　Optional Header …… 69
3.1.4　节表和节 …… 70
3.2　PE 病毒原理研究 …… 71

3.2.1 重定位技术 …… 72
3.2.2 获取 API 技术 …… 73
3.2.3 搜索感染目标技术 …… 74
3.2.4 内存映射 …… 74
3.2.5 感染 PE 文件技术 …… 75
3.3 PE 病毒采用的高级技术 …… 77
3.3.1 加密技术 …… 77
3.3.2 多态技术 …… 77
3.3.3 变形技术 …… 77
3.4 虚拟化技术应对病毒自修改代码 …… 78
3.5 Windows 文件系统过滤驱动 …… 80
3.6 实验分析与验证 …… 90
3.7 本章小结 …… 93

第 4 章 摆渡木马主动防御框架 …… 94

4.1 摆渡木马主动防御框架 …… 94
4.1.1 设计目标 …… 94
4.1.2 设计思想 …… 94
4.1.3 主动防御框架 …… 97
4.1.4 监控模块设计 …… 101
4.2 行为捕获技术和行为特征 …… 102
4.2.1 Windows API 钩子技术 …… 104
4.2.2 木马的不可精确判定性 …… 105
4.2.3 朴素贝叶斯分类算法 …… 106
4.3 环境检测 …… 109
4.4 木马检测评判标准 …… 111
4.4.1 测试指标 …… 112
4.4.2 ROC 曲线 …… 112
4.5 实验与分析 …… 114
4.5.1 实验目的与环境 …… 114

4.5.2 训练集与测试集 …… 115
4.5.3 实验结果与分析 …… 115
4.6 本章小结 …… 117

第 5 章 检测与清除模块设计 …… 118

5.1 功能描述 …… 118
5.2 逻辑流程 …… 120
5.3 文件扫描与检测技术 …… 123
5.3.1 PE 文件扫描与检测 …… 123
5.3.2 压缩文件检测与扫描 …… 124
5.3.3 其他类型文件的检测与扫描 …… 126
5.4 文件隔离与删除技术 …… 127
5.5 恶意文档检测与删除技术 …… 129

第 6 章 特种木马防护模块设计 …… 133

6.1 功能描述 …… 133
6.2 逻辑流程 …… 134
6.3 动态防御注册表驱动过滤 …… 135
6.4 动态防御文件驱动过滤 …… 142
6.5 动态防御网络协议驱动过滤 …… 146
6.5.1 TDI 过滤简述 …… 146
6.5.2 具体过程 …… 148
6.6 动态防御进程驱动过滤 …… 151

第 7 章 特种木马特征库设计 …… 154

7.1 模块描述 …… 154
7.1.1 植入阶段的行为特征分析 …… 155
7.1.2 安装阶段的行为特征分析 …… 155
7.1.3 运行阶段的行为特征分析（文件访问、回联） …… 156
7.1.4 通信阶段的行为特征分析 …… 157

7.2 特征库组成……157
7.3 特征库加载……162
7.4 自定义特征库……164
7.5 行为规则库……166

第 8 章 系统演示和总结 …… 168

8.1 功能描述……168
8.2 系统操作描述……168

附录 示例代码 …… 177

1-1 探测有移动存储介质接入系统 …… 177
1-2 DLL 木马注入演示示例 …… 178
1-3 Toolhelp API 枚举系统进程 …… 182
1-4 PSAPI 枚举进程信息 …… 183
1-5 隐藏模块的方法 …… 185
1-6 自删除示例代码 …… 187

参考文献 …… 189

第1章 绪 论

1.1 背景及意义

随着互联网技术突飞猛进的发展，政府机构、企业工业、教育、国防等领域也逐步信息化，网络在为人们提供极大便利的同时，也带来了计算机信息网络的安全问题，病毒、木马的频发造成信息失窃、经济受损，给国家和网民都带来了巨大的损失。2011 年 2 月 16 日，金山网络发布了《2010—2011 年中国互联网安全研究报告》，报告显示 2010 年新出现了 1798 万多种病毒木马。从图 1.1 可以看出，绝大部分的恶意程序仍然是近几年最主流的木马，其次是后门程序和传统病毒，由于软件的漏洞保护越来越受到重视，蠕虫所占比例是最低的。新增的木马主要分为绑架性木马和网购木马两类。如今的黑客攻击不再满足于使系统崩溃来展示自己的技术，而是转向窃取经济利益。随着电子商务行业的飞速发展，网上购物逐渐普及，黑客瞄准了这个有利可图的领域，制造出了很多专门针对网购人群的木马，给商家和用户造成了严重的损失。

木马是黑客用来盗取受控计算机中信息的一种程序，甚至可能远程控制对方的计算机，以达到盗取密码、机密资料等各种数据的目的。现在的木马不再像以前的盗号木马那样仅仅是为了盗取游戏币等虚拟财产，而是在目标系统中进行配置来为某些网站刷流量，或为某些商业软件做广告来获取费用。可见木马对网络信息安全已经构成了严重的威胁和危害，是造成个人、企业和国家信息泄露的主要途径之一。因此，国家保密局宣布把“对特种木马的检测和对

互联网的保密检查”确定为目前保密科技研究和保密检查的重点关注方向。

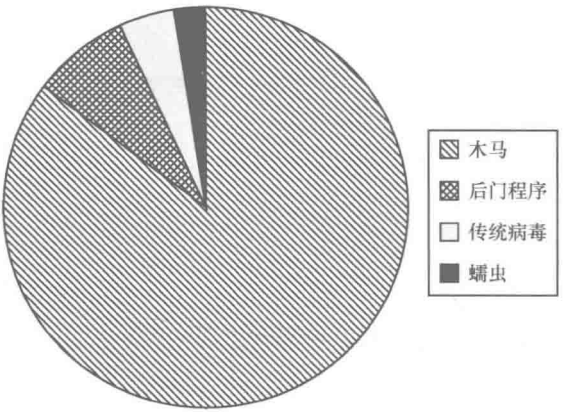

图 1.1　2010 年恶意程序的组成比例

政府单位、军工部门、银行等重要机构为保证信息系统的安全，通常会将单位内网（涉密信息系统）与外网（互联网）进行严密的物理隔离，确保涉密网络不以任何途径与公共互联网相连。涉密信息系统需严格遵守“涉密不上网，上网不涉密”的保密管理规定。虽然物理隔离措施很大程度上阻止了来自外网的病毒、木马等恶意程序的直接攻击，但是并没有完全解决涉密计算机信息系统的安全问题，离线交换文件数据的工具（如 U 盘、光盘）给涉密信息系统带来了很多潜在的威胁。最典型的就是特种木马，它是一种专门通过离线摆渡窃取涉密信息和敏感数据的攻击手段。特种木马作为实施攻击的载体，可以通过移动存储介质与主机之间的数据存取动作完成攻击，首先植入涉密宿主机，然后逐步窃取整个涉密信息系统内的敏感数据，最后通过反向链接和数据中转向远程控制端发送数据，从而完成整个攻击过程。特种木马是一种为间谍人员专门定制的特种程序，对涉密内部网络具有很大的攻击性和破坏性，而且由于其专用性、针对性和未知性，使现有的杀毒软件和防火墙都面临着极大的考验，在这样的背景下主动防御技术的研究就显得势在必

行[1]。研究攻击者使用的工具、手段和攻击方式，及时发现未知病毒和木马，变传统的被动防御为积极的主动防御才是最有效的防护措施。

早在21世纪初期，在我国的涉密网络内就发现了摆渡木马；接着，在后续的安全保密检查过程中，相关人员在很多涉密网络内部都发现了不同类型的摆渡木马，这些木马的攻击意图和行为方式都具有差异性，且行为私密难以发现。很多国家安全部门、科研院所因遭受到摆渡木马的攻击，使大量涉及国家核心利益的信息被非法窃取，给国家的政治安全、社会稳定造成了非常严重的威胁，造成了巨大的经济损失。2011年以来，国家网络安全部门接到的来自各级政府、企事业单位受到摆渡攻击的通报数量直线上升，因被植入摆渡木马而造成的信息泄密事件时有发生，给国家安全带来了不可估量的严重后果。

特种木马作为实施攻击的重要载体，可以通过涉密移动介质间的数据存取完成攻击，植入涉密宿主机，并逐步掌握整个涉密网络内的相关数据，再通过反向链接和多次数据中转将数据向外发送，完成整个攻击过程。作为一种间谍人员定制的特种程序，特种木马对涉密信息系统具有极强的攻击性和危害性；一旦特种木马进入涉密信息系统，其对国家信息安全所产生的危害不可估量。

1.2 木马的检测与防护

在信息安全领域，特洛伊木马（简称木马）是一种后门程序，是黑客为了盗取计算机用户的个人信息、甚至远程控制对方的计算机而加壳制作的，然后通过各种途径传播或诱骗用户执行该程序，从而达到盗取账号密码等各种重要数据资料的目的。木马程序技术的发展非常迅速，在数据传递技术和进程隐藏方面都有了很大改进。现在比较高级的是驱动级木马，这种木马使用了大量的Rootkit技术来达到深度隐藏的目标，并且深入到内核空间，增加

了查杀难度。摆渡木马是一种新出现的特种木马，专门针对内网环境，体现了木马发展的专攻性。有攻就有防，与此同时，木马检测技术也在不断进步，由传统的特征码技术逐渐发展到目前流行的入侵防御技术。

1.2.1 特种木马的基本特征

作为涉密信息系统，在信息处理方式、应用环境设置、安装软件类型、用户操作行为等方面都有其特殊性和代表性。例如，被处理信息的内容多以文本类、图片类电子文件为主，同时包含部分视频以及音频文件。

从目前涉密信息系统的建设情况及安防措施来看，作为一个封闭式的涉密信息系统管理模式，其与外界进行数据交互的方式十分单一，且要求严格，即中间机、光盘、涉密专用存储介质 3 类。因此，能够进入涉密信息系统的特种木马也必然具有其特有的静态特征与动态特征，这些特征在特种木马生命周期（植入、传播、隐藏、启动、窃取、发送）的各个环节都有具体体现。

摆渡木马是一种摆渡类的特种木马。2006 年 4 月国外某杀毒厂商截获了一种专门针对移动存储介质的木马，这种木马隐藏于 U 盘、光盘等移动存储介质中，当感染了此木马的移动存储介质连接到内网中的计算机后，就将木马植入被接入的计算机中，木马搜索该计算机中的文件数据并收集感兴趣的目标文件，随后打包并悄悄发送到 U 盘。这一切都是在用户没有察觉的情况下进行的，可见摆渡木马的隐藏功能足够强大。一旦该移动存储介质接入外网，就会将其收集到的文件、数据等信息通过互联网向外界发送。由于此种木马的攻击方式就像摆渡人通过渡船把乘客摆渡到河对岸，因此被形象地称为“摆渡木马”。 这里，U 盘、光盘等移动存储介质就是“渡船”，窃取的信息就是“渡客”。

以摆渡类特种木马为例，其全生命周期运行流程如图 1.2 所示。在 U 盘、光盘为摆渡载体的情况下，该类型木马包含了植入、隐藏、自启动、数据搜索、文件发送以及自我销毁等核心环节。

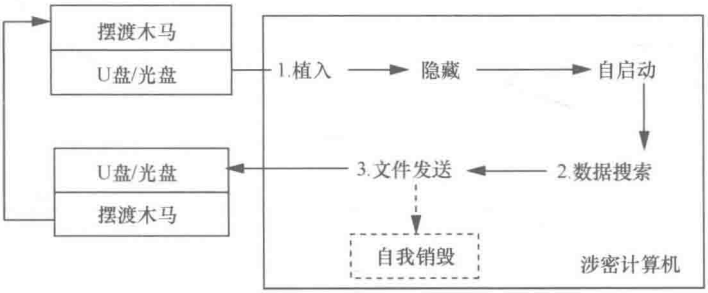

图 1.2 摆渡木马运行的生命周期

系统在设计上充分结合涉密信息系统所采用的操作系统平台、应用软件种类、用户行为方式以及涉密信息系统管理守则，制定符合涉密信息系统特点的特种木马静态生存特征。

采用逆向推理手段，面向特种木马生存需求环境，针对特种木马生命周期中的各个环节，分析木马侵入涉密信息系统的动态行为特征。同时，采取主动跟踪方式，搜集和捕捉特种木马动态行为特征。

1.2.2 特种木马隐藏技术

众所周知，一个病毒木马进入计算机系统的首要任务是保护自己不被杀毒软件、防护系统或用户所发现，即使被发现了也要想办法使自己不被查杀掉，只有存活下来，才有机会实现窃取信息的任务。所以对木马的隐藏以及免杀的研究是非常重要的工作。

前些年比较常见的木马文件隐藏方式是将木马病毒伪装成本地文件。木马病毒将可执行文件伪装成图片或文本，在程序中把图标改成 Windows 的默认图片图标，再把文件名改为.JPG 或.EXE。由于 Windows 默认设置是不显示已知的文件后缀名，文件将会显示为.JPG，不注意的人一点击这个图标就在无意间启动了木马程序[2,3]。

利用配置文件的特殊作用，木马很容易就能在计算机中运行。如 autoexec.bat 和 Config.sys。像 DOS 在启动会自动运行