学校编码：10384　　分类号_____密级_____
学号：X2010230694　　UDC_____

厦门大学

工 程 硕 士 学 位 论 文

面向国税系统的 Fast-Flux 僵尸网络检测系统的设计与实现

The Design and Implementation of Fast-Flux Based Botnet Detection System For National Taxation System

陈维维

指 导 教 师：刘 昆 宏 副 教 授
专 业 名 称：软 件 工 程
论文提交日期：2012 年 10 月
论文答辩日期：2012 年 11 月
学位授予日期：　　年　　月

答辩委员会主席：_____
评　　阅　　人：_____

2012 年 11 月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下,独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行)》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名)：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　√　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

摘 要

我国税收信息化建设历经 20 多年的努力，形成了基本涵盖税收业务、行政决策、公文处理、外部连接四大方面的信息系统，数据正在向省局及总局一级集中处理，形成了从国家税务总局到县级税务局的四级专线网。因此，如何检测网络入侵，有效跟踪追查不法分子和俘获有害信息已经成为一项迫切的新课题。

本文以国税系统僵尸网络检查为应用背景，研究面向国税系统的 Fast-Flux 僵尸网络检测系统的设计与实现。主要内容简单归纳如下几点：

（1）阐述了本文研究的背景和意义，概述了国税系统网络安全现状，为进一步研究僵尸网络奠定了基础。

（2）介绍了有关僵尸网络的概念及理论方法，阐述 Fast-Flux 的相似概念、分类、研究方法以及系统设计的相关理论，为进一步研究 Fast-Flux 僵尸网络检测系统的设计与实现奠定基础。

（3）进行系统需求分析，同时介绍了五种典型的僵尸网络检测体系结构，并结合国税系统特点设计本系统，建立了包含数据预处理与存储系统、对比验证系统和结果展示平台三部分组成的系统模型。

（4）对检测系统性能进行了测试和分析，给出了测试结果。

该系统的设计与实现，能够实时对国税系统内部网络进行监控，简化了税务网络安全管理人员对网络安全的监测工作，预防了 Fast-Flux 型僵尸网络的入侵，在建设国税系统网络安全体系中发挥了重要作用。

关键词：国税网络；Fast-Flux 僵尸网络；检测系统；

Abstract

With the continuous efforts over the past 20 years, it has gained primary efficiency on saturation of taxation information system in China. An integral information system has been constructed and it covers fours sections including revenue business, administrative decision, document handling and external connection. Data are collected for concentrated handle. Four-level private network from the State taxation of Administration taxation Bureau has been constructed, through which all data is transmitted. It becomes an urgent request to strengthen the security consumption of network and the whole information system, and it takes great realistic sense to research completely, systematically and scientifically on the networks security of the system.

This dissertation takes the Botnets of the national tax system as application background, thus, the national tax system Fast-Flux Botnets detection system is designed. Main contents are briefly summarized as follows.

(1) The background and significance has been elaborated overview of the network security status of the national tax system, including the course of development of botnet, botnet definition, the control mechanism of the functional structure of the bots and botnet, and internal mechanism of tracking, defense, counter and the check methods.

(2) Concept of botnet theory is introduced. The similarity of the concept of Fast-Flux, Fast-Flux research methods and system design theory are described in detail for further research. And the Fast-Flux Botnet detection system design and implementation of the foundation is also introduced.

(3) Fast-Flux Botnet detection system based on the national tax system modeling is introduced, along with the basis and call library. In this part, Five typical hierarchical framework detection architecture, generic detection framework architecture, multilayer architecture, integration framework architecture based ISP collaborative botnet detection framework detection architecture are firstly introduced, containing data preprocessing systems, storage systems, sniffing acquisition, web interface part of the system model. Contrast verification system structure description, flow charts, and display platform.

(4) The performance of Fast-Flux Botnet detection system based on national tax system is tested and analyzed along with our conclusions.

The implement and application of this system can realize the management of realtime security for the intranet of the national tax system. It relives the work burden of the

network security management department, and plays an important role in the national tax system security network.

Keywords： National Tax Network; Fast-Flux Botnet; Detection System

目 录

Contents

第一章 绪论

国税部门属于国家税收管理、国家财政收支的政府重要职能部门。伴随着社会主义市场经济的发展，国家税收扮演了财政收支、经济调控、社会分配调节等职能。因此，国税系统的信息化对于增加税收管理效率、制定合理税收政策甚至对于推动整个国民经济发展具有极其重要的作用。近年来，在网络结构上国税系统相应形成了外部局域网和内部广域网两套网络体系，日常工作中无法避免访问互联网，因此，国税系统的网络安全问题也将被带入内部网络中，而国税系统的内部广域网络与外部银行、互联网、工商、国库等网络连接，从而对国税系统的网络安全提出了更高的要求。然而，随着计算机应用技术的不断发展，特别是僵尸网络的肆虐给国税系统网络带来了更大的威胁，人们对国税系统网络的安全性、可靠性等性能要求不断提高[1]。国内外有关研究表明，僵尸网络普遍采用 Fast-flux 技术，从而使得研究面向国税系统的 Fast-Flux 僵尸网络检测系统成为国税系统网络安全领域的热点研究课题。

1.1 研究背景及意义

随着通信技术的快速发展，特别是互联网技术的发展，已经改变了传统的通信方式、社会组织管理和人际沟通方式，并且还极大地影响了人们的社会生活和政府的有关运作方式。我国国税系统以“金税工程”的发展建设为契机，使用了现代的信息技术来处理国税信息，构建了以信息化管理为核心的现代税务管理体系，获得了较好的社会和经济效益。随着信息技术的发展，我国国税信息化建设不断完善，其发展轨迹可划分为以下四个阶段：第一阶段(1982-1989)是税收电子化初始阶段，也称为模拟手工的电子阶段，其总体技术特征通常为采用数据库技术，依托局域网和单机，涉及税务应用的操作层次，对税收业务的重要环节实现了手工操作的计算机化。第二阶段(1990-1993)是步入面向管理的税收管理信息系统阶段，其总体特征为采用关系型数据库、客户机/服务器模式及图形化界面，依托广域网进行分布式处理，涉及税务应用的操作和管理层次。第三阶段(1994-2000)是实现创造税收价值的全方位税收服务系统阶段，其总体特征为采用 Web 技术和组件化结构，依托互联网实现集中式处理，涉及税务应用的操作、管理和决策层次，并对纳税人进行全面的

管理与服务。第四阶段(2000~)税务管理信息一体化建设阶段。实行统一规范的应用系统平台，依托税务系统计算机广域网，建立覆盖各级税务机关行政管理、税收业务、决策支持、外部信息应用等所有职能的功能齐全、协调高效、信息共享、监控严密、安全稳定的信息系统[2]。

最初，互联网基本上是一个不设防的网络空间，其采用的 SNMP、TCP/PI 等协议的安全性比较弱。它强调共享性和开放性，自身并不为用户提供较高的安全保护。随着互联网技术的快速发展，近年来，国税人员的计算机素质也得到飞速的提高，目前，我国国税系统大都是建立在基于 Web 服务的三层结构体系之上的，这也从技术层面上对国税系统的网络及系统安全上提出了更高的要求。

研究表明，僵尸网络是隐秘操纵分布式拒绝服务（Distributed Denial of Service, DDoS）攻击、垃圾邮件（Spam）、网络钓鱼攻击（Phishing）、窃取敏感信息等恶意活动的“元凶”。僵尸网络，集合了传统的恶意软件（如网络蠕虫、木马以及计算机病毒等），变为一种可控的、能够发动各种恶意活动的平台。

通过僵尸网络技术，操作者可以轻易的控制主机，从而导致僵尸网络的规模扩张。如图 1.1 所示，为 2010 年 8 月赛门铁克公司发出的僵尸网络全球分布图，图中深色边圆点代表僵尸网络分布广度位居前 10 位，带浅色边圆点代表僵尸网络分布广度位居 11 到 50 位。由图可以看出僵尸网络几乎存在于世界上的每个角落中。又如图 1.2 所示，2007~2009 年赛门铁克公司的监测数据表明，僵尸主机（Zombie）数量每天都达到了几万台，每年识别出的命令与控制服务器（Command and Control, C&C）的数量迅速增长，而且综合观察得到的各种僵尸主机数量达到几百万台/年，甚至接近一千万台/年。根据迈克菲公司安全威胁报告，2010 年第二季度在全世界范围内检测到约 1500 万台计算机感染了僵尸网络，其中印度的感染数量近 150 万台，巴西、俄罗斯和德国的感染量也超过了 100 万台[3]。由于僵尸网络的隐蔽性比较强，实际僵尸主机的数量肯定远大于报告中的数量。如果牟取经济利益的攻击者手掌握了僵尸网络，不仅会对互联网运行和社会经济造成重大危害，更会产生日益严重的网络犯罪。当前所有的 DDoS 攻击都是由僵尸网络平台发起的，95%以上的垃圾邮件也来自僵尸网络，而网络钓鱼攻击和信息窃取更是僵尸网络的专长。然而针对于我国国税系统的 DDoS 攻击造成的经济损失动辄就达上百万美元。国际电信联盟（ITU）曾统计垃圾邮件每年给世界经济造成的损失高达 250 亿美元，图 1.3 给出

了全球垃圾邮件数量及其占邮件总数的比例。据调查显示，2007 年网络钓鱼攻击给美国带来的损失已上升到 32 亿美元，在该年 8 月份之前的 12 个月期间大概有 360 万成年人被网络钓鱼攻击所欺骗。2010 年 9 月，攻击者利用 Zeus 僵尸网络感染了全球各地的计算机，以便窃取密码、银行账号和用于登录网上银行账户的其他数据，从而可在未经授权情况下每次转移数千美元，最终该案件被联邦调查局（FBI）侦破，涉及英国、美国、荷兰、乌克兰等国，企图窃取金额 2.2 亿美元，实际损失 7000 万美元。

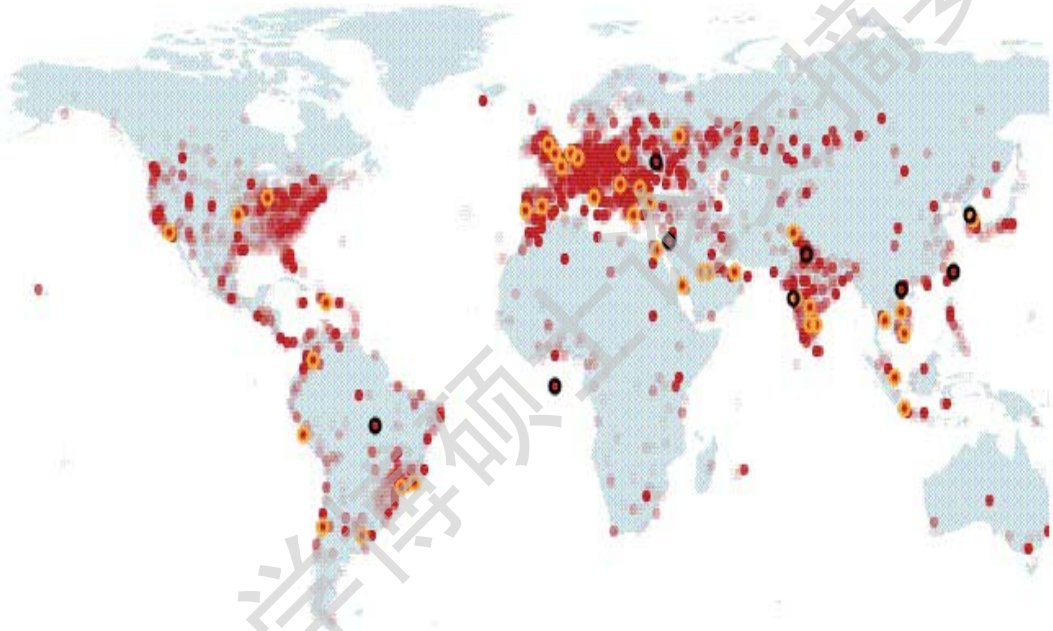

图 1.1 僵尸网络全球分布情况

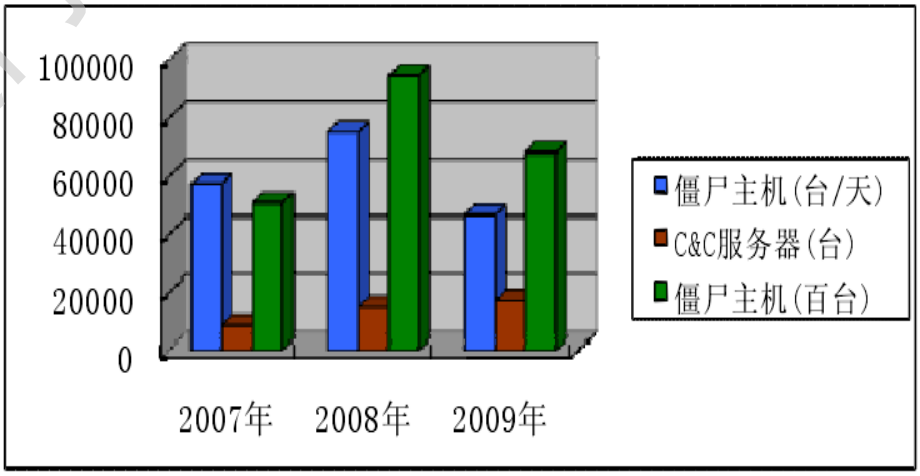

图 1.2 赛门铁克公司监测数据情况

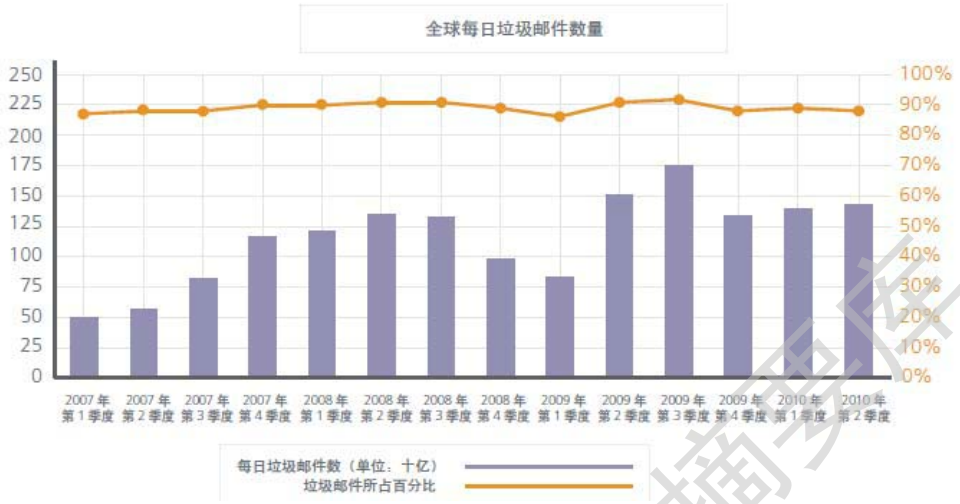

图 1.3 全球垃圾邮件数量及其占邮件总数的比例

目前，我国早已成为最大的僵尸网络受害国之一，中国大陆被僵尸网络控制的主机数量占全世界总数量的比例多次超过美国，引起了政府机构和网络用户的高度重视。2010 年，我国国家计算机网络应急技术处理协调中心（CNCERT/CC）公布[4]：全年共发现近 500 万个境内主机 IP 地址感染了僵尸程序，较 2009 年大幅增加，具体分布情况如图 1.4 所示；某些政府网站、腾讯业务系统以及游戏服务器等遭受到多次 DDoS 攻击，对公共互联网的安全运行造成了较大冲击；中国垃圾邮件的数量仍然占到全球垃圾邮件总量的一定比例。

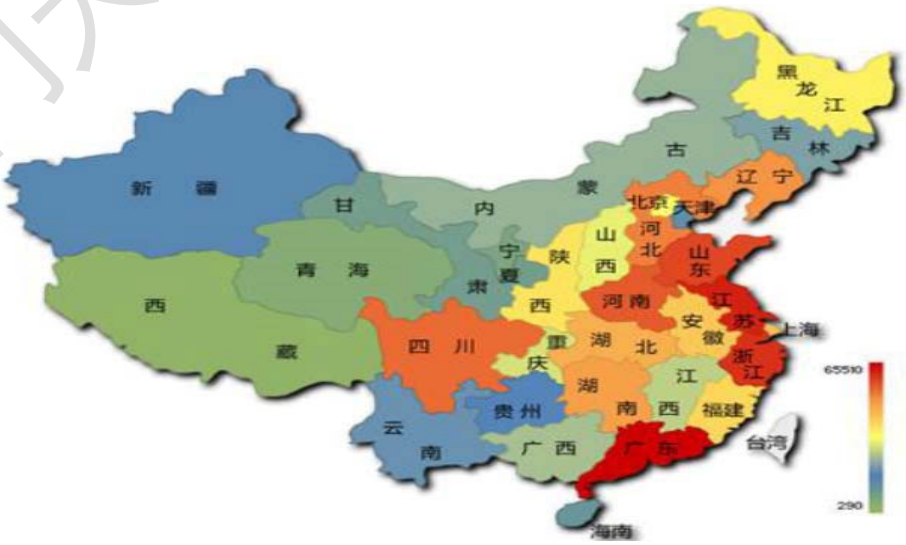

图 1.4 僵尸网络受控主机在我国大陆的分布