doi: 10.3969/j.issn.1006-1576.2012.10.015

涉密信息系统的防病毒木马方法

糜旗，胡麒，宗俊珺
（中国航天科技集团第八研究院上海航天动力技术研究所，上海 201109）

摘要：针对军工单位涉密信息系统的安全保密技术防护现状，对病毒木马的防治方法进行研究。介绍现有涉密信息系统的防病毒木马软件的原理和关键技术，分析了防病毒木马软件的不足，介绍一种自行开发的病毒木马辅助查杀软件，并通过部署多维化防病毒木马体系、涉密信息系统入口的防毒流扫描技术、其他辅助手段以及加强安全保密工作等手段对病毒木马进行防治。结果证明：军工单位应该将病毒木马防范技术和安全保密管理工作结合起来进行常态化管理，才能确保涉密信息系统的安全可靠。

关键词：涉密信息系统；病毒；木马
中图分类号：TJ03 **文献标志码**：A

Method of Anti-Virus and Anti-Trojan in Secret-Involved Information System

Mi Qi, Hu Qi, Zong Junjun
(*Research Institute of Shanghai Aerospace Power Technology*, *No*. 8 *Academy of China Aerospace Science & Technology Corporation*, *Shanghai* 201109, *China*)

Abstract: Aiming at the defense situation of security and secrecy in the secret-involved information system, research the methods of anti-virus and anti-Trojan. Introduce the current principle and key technology of anti-virus and anti-Trojan software in the secret-involved information system, analyze the shortage of anti-virus and anti-Trojan software. Introduce a self-defined anti-virus and anti-Trojan assistant software, prevent the virus and Trojan through deploying dimensionalities anti-virus and anti-Trojan system, anti-virus scanning technology in the entrance of secret-involved information system and other assistant instrument to enhance security and secrecy. The result proves, the armament industry shall combine the anti-virus and anti-Trojan technology and security and secrecy works, manage normalization to affirm the safety and credibility of secret-involved information system.

Key words: secret-involved information system; virus; Trojan

0 引言

病毒与木马都是人为编写的代码或程序，都属于电脑病毒范畴。病毒最通常的定义可以表述为：“利用计算机软硬件所固有的弱点编制的具有自身复制能力的、会不断感染的、具有特殊目的的计算机程序”。编写病毒的目的除了破坏数据之外，有些则是为了获取利益或炫耀技术。木马全称为“特洛伊木马程序”，通常是指伪装成另一正常程序或隐藏在正常程序中的一段具有特殊功能的恶意代码，它入侵计算机后会悄悄打开某个端口，接受使用者的远程控制，即木马的作用是在隐蔽、非授权的计算机环境中偷窥隐私和盗窃数据。因此，笔者将木马从病毒类型中剥离出来，单独称之为“木马”或“后门”。目前，军工企业涉密信息系统中防病毒木马的主流方法是安装具有涉密产品资质证书国产防病毒木马软件，例如瑞星、江民等，很难有效地防御病毒木马的入侵、传播、感染和爆发，尤其当遇到某些未知或特种病毒木马，更是一筹莫展。在病毒木马日益泛滥的时代，军工企业防病毒木马的形势越来越严峻，对涉密信息系统的安全保密提出了越来越高的要求。笔者基于涉密信息系统的具体要求，对病毒木马的防治方法进行研究。

1 计算机病毒木马产生背景

计算机病毒木马的产生是计算机技术和以计算机为核心的社会信息化进程发展到一定阶段的必然产物。它产生的背景是：

1) 计算机病毒木马是计算机犯罪一种新的衍生形式，它取证困难、风险小、破坏大，属于高科技犯罪。具有动态性、瞬时性和随机性的特点。

2) 计算机属于电子设备，数据在输入、储存、处理、输出各环节都容易发生篡改、丢失、伪造和损坏的情况；程序代码容易被修改删除，至今仍没有办法事先知道有多少错误和缺陷隐藏在程序代码中，只能在运行中发现和修改错误。这些脆弱性就为病毒木马的入侵提供了方便。

收稿日期：2012-05-09；**修回日期**：2012-06-12
作者简介：糜旗(1979—)，男，上海人，工学学士，工程师，从事网络与信息安全、计算机逆向工程研究。

3) 涉密信息系统中局域网的建设和计算机的普及是计算机病毒木马产生的必要环境。病毒木马感染传播的能力和途径也由原来的单一变得复杂隐蔽，尤其是局域网环境的复杂化，为病毒木马生存提供了最快最好的温床。

2 涉密信息系统安全保密现状

近年来，国家对武器装备科研生产单位开展了保密资格认证工作，尤其对涉密信息系统提出了极高的要求，因为涉密信息系统中承载大量的国家秘密信息[1]，围绕科研生产和日常办公两类业务，涉及财务资金管理、OA 办公、计划管理、人力资源管理、协同设计和生产制造等。

但时至今日，军工单位对于涉密信息系统技术防护不到位的问题仍然非常突出，面对日益严峻的保密形势，信息泄密、网络崩溃的事件时有发生，无法有效保障国家秘密的安全。例如：

●个别内部人员利用病毒木马实施越权访问，窃取国家秘密；

●违规外联行为、移动存储介质的管理疏漏使得从外部间接入侵和引入病毒、木马成为可能；

●蠕虫病毒的泛滥造成数据被破坏和篡改，造成涉密信息系统瘫痪。

而这些事件的诱因，很大程度来自于病毒木马。根据某国内防病毒厂商的估算，仅在 2011 年，针对涉密信息系统的攻击事件就高达 10 万次以上，其中 90%的攻击 IP 地址来自国外，美国、日本、韩国是排行最前的 3 个攻击来源地，如图 1。

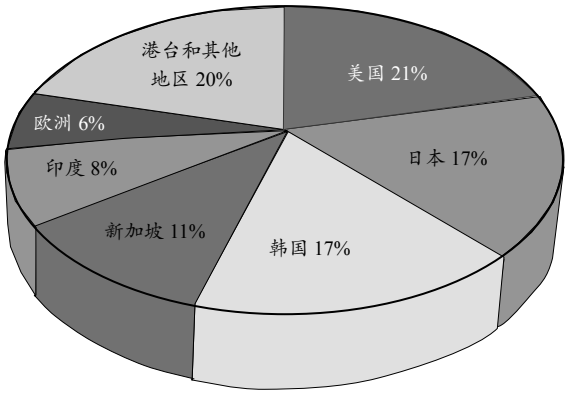

图 1 对涉密网络发动攻击的 IP 来源

3 涉密信息系统防病毒木马软件概述

3.1 防病毒木马软件的原理

防病毒木马软件一般由扫描器、病毒库与虚拟机组成，并由主程序将它们结为一体。扫描器是防病毒木马软件的核心，通过扫描文件、扇区和内存等发现病毒木马。不同的功能对应着不同的扫描器，所以防病毒木马软件都是由多个扫描器组成的。病毒库用于存储病毒木马的特征码[2]。虚拟机可以使病毒木马在一个由防病毒木马软件构建的虚拟环境中执行，与现实的 CPU、硬盘等完全隔离，从而可以更加深入地检测文件的安全性。

3.2 防病毒木马软件的技术

3.2.1 特征码技术

特征码是识别一个病毒的一段不大于 64 字节的特征串。发现新病毒木马后，通过分析提取出特征串，编成特征码，添加到数据库。以后在进行查杀过程中，通过比对文件特征串与数据库中的特征码，检查文件是否含有病毒木马[3]。针对传统病毒木马查杀，特征码技术有扫描速度快，误报率低，资源占用最小的特点。大多数防病毒木马软件都配备有特征码扫描引擎，这也是最常用的技术。

3.2.2 虚拟机技术

虚拟机技术具有人工分析、高智能化、查杀准确性高等特点。该技术的原理是：用程序虚拟 CPU 环境，包括硬件端口，用调试程序将病毒木马在虚拟环境中激活执行，通过内存、寄存器以及端口变化来了解程序的任何动态，根据其行为特征，从而判断是否为病毒木马[4]。避免了在真实系统环境中调试分析样本，而感染破坏系统的状况。

3.2.3 主动内核技术

主动内核技术就是将已经开发的各种防病毒木马技术从源程序级嵌入到操作系统或网络系统的内核中，与其浑然一体，如同给系统打了一个补丁，而且是一个“主动”的补丁[5]。这种技术可以保证防病毒木马模块从底层内核拦截所有的文件访问，确保在发现病毒木马入侵时，在内存阶段即被截获并作出处理，解决目前防病毒木马软件普遍难以查杀驱动型病毒木马的技术难题。

3.3 防病毒木马软件的不足

随着计算机技术和网络的不断发展，特别是变形病毒和特种木马的种类增多，致使防病毒木马软件缺陷越来越明显，无法准确报警，查杀效率下降，主要表现为以下几个方面：

1) 传统防病毒木马软件只能针对本地系统进行防御，基于文件进行扫描的查杀方式效率极低，无法适应对效率要求极高的网络查毒。特别是很多

病毒木马是专门针对某个企业编写的，感染传播速度极快，而且很难阻止和清除。

2) 主流的病毒木马查杀技术主要是采取匹配特征码方式。根据防病毒木马软件的机理，特征码库升级是永远晚于病毒木马传播的，这使防病毒木马软件对未知病毒木马无能为力。等发现病毒木马时，信息已经被破坏，秘密已经被窃取[6]。经笔者测试，对已能查杀的病毒木马进行变形加壳或添加汇编花指令后，防病毒木马软件就无法正常识别查杀生成的新变种。

3) 虚拟机技术的弊端是高系统资源占用，甚至有时候会导致防病毒木马软件和操作系统出现假死现象。

4) 主动内核技术的弊端是容易出现误报现象，这种弊端在很长一段时间内将无法克服，使用这种技术存在一定程度的风险，一旦涉密信息系统某个关键的合法应用程序被误报删除，将是灾难性的[7]。笔者单位曾遇到防病毒木马软件将所有计算机终端的 IE 浏览器误报为病毒，然后全部删除，造成所有终端无法上网。

5) 病毒加密。病毒木马采用可执行文件加密压缩和反跟踪技术之后，导致出现大量的变形病毒，这对病毒木马的分析查杀更困难。

6) 从国外进口的很多软硬件不掌握自主知识产权。由于无法查看底层代码，所以软硬件可能会存在有意留下的漏洞和编写精巧的“特种木马”。对于这类代码程序，防病毒木马软件通常都毫无办法。从编程风格、操作精细程度和利用的漏洞质量等多方面观察，很可能是国外有组织有目的的情报收集和破坏活动。例如 2010 年 9 月，“超级工厂 (stuxnet)”病毒是全球第一个能真正破坏工业自动化系统的病毒。有媒体报道说，该病毒是由美国情报部门协助以色列制造的，在伊朗散播后防病毒木马软件未能及时查杀，病毒发作时造成极其严重的后果，遭病毒攻击的核电站有数千台离心机运行异常，使得伊朗核计划遭到挫败。

4　防病毒木马的方法

4.1　建立特定病毒木马特征码库

由于上述防病毒木马软件的种种先天不足，建议可以自行开发病毒木马辅助查杀软件，通过建立本单位特定的未知病毒木马特征码库，来提高病毒木马的查杀率[8]，如图 2。

图 2　自行开发病毒木马辅助查杀软件

例如：笔者单位使用主机审计系统、防火墙和入侵检测系统等安全保密产品对网络数据包和计算机终端进行实时预警跟踪审计，一旦发现活跃的异常程序，使用调试器进行反汇编分析，如图 3。

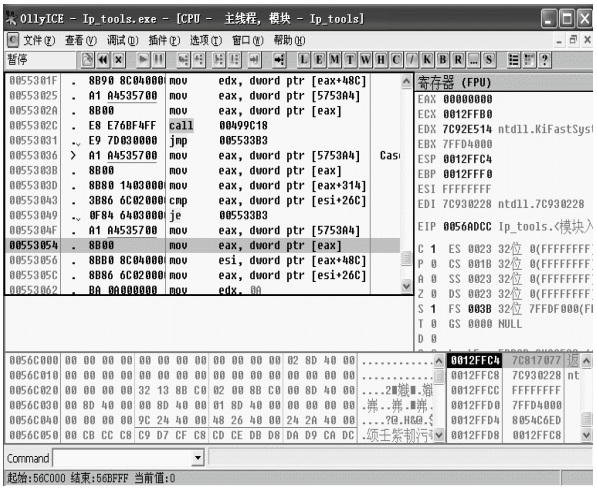

图 3　使用调试器进行反汇编分析

如果确认异常程序具有恶意代码段，则将程序的特征码并加入自行开发的航天特种木马病毒专杀工具的数据库中，如图 4。

图 4　航天特种木马病毒专杀工具数据库

4.2 部署多维化防病毒木马体系

涉密信息系统的防病毒木马要跳脱出传统单机的严防死守，立足于整个网络的统一联防，再重点建设全网多维安全，从简单查杀的孤岛战略延伸为多维化防病毒木马架构，将防病毒木马安全基线从涉密计算机扩展至涉密网络，再延伸至网络节点的边界设备，从安装单一软件扩展到部署多种软硬件，打造出由防病毒木马软件、交换机、防火墙、入侵检测系统和主机审计系统等组成的“混编舰队”。

4.3 涉密信息系统入口的防毒流扫描技术

为了能进一步降低病毒木马进入涉密信息系统的概率，入口处的防病毒木马方案越来越被广泛采用。它主要是对进出涉密信息系统的数据和行为，在入口处进行检查，争取第一时间就可以检测出病毒木马并及时清除，有效避免病毒木马进入涉密信息系统。

由于涉密信息系统入口防毒一般都在网络入口处进行，因此对病毒木马查杀效率提出相当高的要求，以避免出现明显的网络延时。于是专门为网络入口防毒而设计的病毒木马流扫描技术应运而生。它对网络流和数据包进行检测，极大降低了系统资源消耗和网络延迟。

4.4 其他辅助手段

在做好防病毒木马软件日常审计工作之余，如果条件允许，可配合国内有实力的网络安全服务商、防病毒木马软件供应商，共同建立防病毒木马巡检制度。即使发生重大安全事故，也可以及时得到专业的技术支持，减少损失，尽快恢复涉密信息系统运行[9]。例如笔者单位就购买了国内某防病毒木马软件公司的金牌服务，每月定期进行安全巡检，及时发现威胁，解决问题，做到防患于未然。

4.5 加强安全保密工作

很多军工单位的安全风险因素来自内部，这些都需要内部建立严格的权限管理体系、资料审核机制和使用登记制度，规范内部员工对计算机终端、移动介质、网络存储和数据摆渡的使用行为[10]，从行政管理方面，最大程度的减少单纯依靠防病毒木马软件无法彻底消除的风险。

首先建立多向性的思维方式，开阔认识问题的视野，校正考虑问题的角度，做到眼观六路，耳听八方，多方面进行探求。

其次是要使保密工作做到有法可依，有章可循。从完善管理制度建设入手，依据《保密法》、《保密资格认证标准》、集团、院、厂所等相关文件的要求，并结合军工单位实际情况，制定切实可行的信息安全保密管理规定。

第三是提高涉密人员素质，特别是在文化业务素质方面，要求涉密人员不仅要懂得传统保密知识，而且还要懂得计算机等高科技条件下的保密知识。

第四是改进保密工作的方法，与时俱进，在探索中学习，在实践中提高，不断提高应对新情况、解决新问题的能力。

第五要突出重点，提高保密技术检查和防范的能力。认真抓好保密管理，认真搞好保密技术装备的配合，经常开展保密技术检查，发现问题，及时清除，把各种隐患解决在萌芽状态。

5 结语

对于军工单位而言，病毒木马的防范应该进行常态化的管理，从保密技术的研究出发，以成功保障涉密信息系统的安全为前提，加强对涉密人员的教育管理，针对不同时期出现的病毒和木马，提高应急响应能力，将保密技术应用到日常的管理工作中，为军工单位的涉密信息系统建设一个安全可靠的环境。

参考文献：

[1] 施峰. 信息安全保密基础教程[M]. 国防科技工业保密资格审查认证中心.

[2] F. Cohen. Computer viruses: theory and experiments[M]. In Proc. 7th National Computer Security Conference, 1984.

[3] C. Young. Taxonomy of computer virus defense mechanisms[M]. In Proc. 10th National Computer Security Conference, 1987.

[4] 王倍昌. 走进计算机病毒[M]. 北京: 人民邮电出版社, 2010.

[5] 侯明明. 浅析“木马”病毒及其防治措施[J]. 广西轻工业, 2009: 3.

[6] 彭伟. 网络信息安全隐患及防范策略研究[J]. 山西师范大学学报: 自然科学版, 2010(01).

[7] 李兆星. 反病毒引擎的自主创新与发展[J]. 信息网络安全, 2010(05).

[8] 惠洲鸿. 计算机病毒传播之数学模型的试建[J]. 西北民族学院学报: 自然科学版, 1999(03).

[9] BMB22-2007 涉及国家秘密的信息系统分级保护测评指南[S].

[10] 国家军工保密资格认证办公室. 军工保密资格审查认证工作指导手册[S]. 金城出版社, 2010.