

# 网络病毒防治技术在计算机管理中的应用

李可 聂昱昕 郭珂琦 唐懋钧 王力  
北京计算机技术及应用研究所 北京 100854

**摘要:** 网络病毒防治技术在计算机管理中至关重要。本文全面分析了网络病毒的特征、传播途径及其危害,探讨了当前计算机管理中应用的网络病毒防治技术,包括安装安全软件、系统更新与补丁管理、数据备份与恢复、网络访问控制及用户安全教育等措施。研究指出,综合应用这些技术能有效提升计算机系统的安全防护能力,减少网络病毒带来的风险。本文为计算机管理提供了实践指导,有助于维护网络安全与稳定。

**关键词:** 网络病毒防治技术; 计算机管理; 应用

引言: 随着信息技术的飞速发展,计算机网络已成为现代社会不可或缺的一部分。然而,网络病毒作为一类恶意软件,不断威胁着计算机系统的安全性和稳定性。计算机管理面临着前所未有的挑战,如何有效防治网络病毒成为亟待解决的问题。本文旨在探讨网络病毒防治技术在计算机管理中的应用,通过深入了解网络病毒的特性和传播途径,提出有效的防治策略,以保障计算机系统的安全运行,为计算机管理提供有力支持。

## 1 网络病毒概述

### 1.1 定义与特征

(1) 计算机病毒的定义。计算机病毒,本质上是一段人为编写的恶意计算机代码程序。它们并非如同生物病毒般存在于实际世界,但其设计初衷和某些特性却与生物病毒有相似之处,尤其是对系统的破坏性和传染性。这些程序并不服务于人们的生产生活,而是对特定的计算机网络或系统进行破坏,以达到盗取数据、私人账户信息等非法目的。(2) 网络病毒的类型。网络病毒的类型多样,根据其功能和传播方式的不同,大致可以分为以下几类: 1) 启动病毒。这种病毒会附着在计算机的启动程序中,一旦计算机启动,病毒就会被激活,进而对系统进行破坏或传播。2) 文件感染病毒。病毒通过感染特定的文件来传播,一旦这些文件被执行,病毒就会被激活,继续感染其他文件或系统。3) 多态病毒。这类病毒具有高度的变异性,能够通过改变自身代码结构来逃避检测,增加了检测和清除的难度。4) 宏病毒。主要攻击使用宏指令的应用软件,如Microsoft Word和Excel等,通过电子邮件附件或文件下载等途径传播。5) 脚本病毒。通常隐藏在网页的脚本中,用户浏览网页时,脚本病毒便会被激活并感染计算机。(3) 网络病毒的主要特征。网络病毒的主要特征包括: 1) 破坏性。病毒会破坏计算机的软硬件系统,导致文件丢失、数据损坏、系

统崩溃等。2) 潜伏性。病毒能够在系统中潜伏很长时间而不被发现,等到满足触发条件时才会爆发。3) 隐蔽性。病毒通常会隐藏自身的存在,避免被检测和清除。4) 传播性。网络病毒能够通过网络迅速传播,感染大量计算机。

### 1.2 网络病毒的危害

网络病毒的危害不容忽视,它们对计算机系统和用户数据安全构成了严重威胁: (1) 破坏文件、硬盘、内存等计算机组件。病毒会破坏计算机的各种组件,导致文件损坏、数据丢失、硬盘分区表被修改等,严重时甚至会导致系统崩溃,无法正常运行。(2) 窃取敏感信息,造成机密泄露。许多网络病毒都具有窃取敏感信息的能力,如窃取用户的账号密码、身份证号、银行卡信息等,这些信息一旦被不法分子获取,就会导致用户隐私泄露,进而引发身份被盗用、财产被盗取等一系列问题。(3) 影响计算机运行效率,甚至导致系统崩溃。病毒在系统中运行会占用大量资源,导致计算机运行缓慢、频繁死机等问题。严重时,病毒还会破坏系统核心文件,导致系统崩溃,无法正常启动和使用。

## 2 计算机管理中的网络病毒传播途径

### 2.1 软件感染

软件感染是网络病毒传播的一种常见方式。许多用户在下载和安装软件时,由于缺乏对软件来源的验证,容易安装到被病毒篡改或捆绑病毒的恶意软件。这些恶意软件在安装过程中会悄无声息地将病毒植入系统,从而实现对计算机的感染。此外,一些看似无害的下载工具、游戏外挂等也可能成为病毒的载体,一旦用户下载并运行,病毒就会随之进入计算机系统。为了防范这一途径的病毒传播,用户应增强安全意识,尽量从正规渠道下载软件,并在安装前仔细阅读软件说明和授权协议。同时,使用可信赖的杀毒软件对下载的文件进行扫

描, 以确保其安全性。

## 2.2 网络传播

互联网是网络病毒传播的主要渠道之一。病毒可以通过网页、链接、下载文件等多种方式在互联网上迅速传播。当用户访问被病毒感染的网页、点击恶意链接或下载带有病毒的文件时, 病毒就会通过互联网进入用户的计算机系统。此外, 一些黑客还会利用系统漏洞进行远程攻击, 直接将病毒植入目标计算机。为了防范互联网传播的病毒, 用户应谨慎上网, 避免访问不明网站和点击可疑链接。同时, 及时更新操作系统和应用程序的补丁, 以修复已知漏洞, 防止黑客利用漏洞进行攻击。此外, 安装可靠的防火墙和杀毒软件也是防范网络病毒的重要手段<sup>[1]</sup>。

## 2.3 电子邮件传播

电子邮件是另一种常见的网络病毒传播途径。病毒可以隐藏在邮件附件或邮件正文中, 当用户打开邮件或下载附件时, 病毒就会被激活并进入计算机系统。一些病毒甚至会伪造邮件发件人地址, 以迷惑用户并诱使其打开邮件。为了防范电子邮件传播的病毒, 用户应谨慎处理电子邮件, 特别是来自不明发件人的邮件。在打开邮件附件之前, 应先进行杀毒扫描, 以确保其安全性。此外, 避免随意点击邮件中的链接, 特别是那些要求输入个人信息或下载附件的链接。

## 2.4 移动设备传播

随着移动设备的普及, 病毒通过USB、SD卡等存储介质传播的风险也在增加。当用户将感染病毒的移动设备连接到计算机上时, 病毒就有可能通过自动播放功能或文件传输等途径进入计算机系统。此外, 一些黑客还会利用移动设备进行恶意攻击, 如通过伪造存储设备植入病毒等。为了防范移动设备传播的病毒, 用户应谨慎使用移动存储设备, 避免将其连接到不受信任的计算机上。在连接移动设备之前, 应先进行杀毒扫描, 以确保其安全性。同时, 关闭计算机的自动播放功能, 以降低病毒通过移动设备传播的风险。

## 3 网络病毒防治技术在计算机管理中的应用

### 3.1 安装专业的安全软件

(1) 杀毒软件与防火墙的部署。杀毒软件和防火墙是计算机安全的第一道防线。杀毒软件能够实时监测和扫描系统, 检测并清除病毒、木马等恶意软件。通过不断更新病毒库, 杀毒软件能够识别并应对最新的威胁。防火墙则能够监控并过滤进出计算机的网络流量, 防止未经授权的访问和数据泄露。在安装杀毒软件和防火墙时, 需要注意软件的性能、版本以及是否正规, 确保能

够提供全面的安全防护<sup>[2]</sup>。(2) 实时监控系统与病毒扫描。除了基本的杀毒和防火墙功能外, 现代安全软件还提供了实时监控和病毒扫描功能。实时监控系统能够持续监控计算机的运行状态, 一旦发现异常行为或潜在威胁, 立即进行报警和处理。病毒扫描则定期对系统进行全面扫描, 查找并清除潜在的病毒和恶意软件。这些功能能够确保计算机系统始终处于安全状态, 及时应对各种网络威胁。

### 3.2 定期更新与升级安全补丁

(1) 操作系统和软件的安全更新。操作系统和软件的安全更新是防治网络病毒的重要手段。这些更新通常包含了对已知漏洞的修复和新的安全防护功能。通过及时安装这些更新, 可以堵塞系统漏洞, 降低病毒入侵的风险。因此, 计算机管理人员应定期检查和安装操作系统和软件的安全更新, 确保系统始终处于最新状态。

(2) 漏洞修复与防护策略。除了安全更新外, 还需要采取漏洞修复和防护策略来增强系统的安全性。漏洞修复包括对系统中存在的已知漏洞进行修补, 以防止黑客利用这些漏洞进行攻击。防护策略则涉及对系统配置的优化和安全策略的制定, 以降低系统被攻击的可能性。这些措施需要综合考虑系统的实际情况和威胁环境, 制定出一套切实可行的安全防护方案。

### 3.3 数据备份与恢复

(1) 定期备份重要数据。数据备份是保护计算机系统安全的重要手段之一。通过定期备份重要数据, 可以在系统遭受病毒攻击或其他意外事件导致数据丢失时, 迅速恢复数据, 减少损失。数据备份应该包括所有重要的文件和数据库, 并确保备份数据的安全性和可用性。同时, 还需要制定备份数据的恢复计划, 以便在需要时能够迅速恢复数据。(2) 数据恢复机制的建立。除了数据备份外, 还需要建立数据恢复机制来应对可能的数据丢失或损坏情况。数据恢复机制应该包括恢复数据的步骤、方法和工具, 以及恢复数据的验证和测试。通过这些措施, 可以确保在数据丢失或损坏时, 能够迅速、准确地恢复数据, 保证系统的正常运行和数据的安全性<sup>[3]</sup>。

### 3.4 网络访问控制与权限管理

(1) 强化网络访问策略。网络访问控制是防止网络病毒传播的重要手段之一。通过制定和执行严格的网络访问策略, 可以控制对网络的访问权限, 防止未经授权的访问和数据泄露。网络访问策略应该包括网络访问的认证、授权和审计等方面, 确保只有合法的用户才能够访问网络资源。(2) 账户权限的合理分配与监控。账户权限的合理分配与监控也是防止网络病毒传播的重要

措施。通过合理分配账户权限，可以限制用户对系统的操作权限，防止用户进行不当操作导致系统被攻击。同时，还需要对账户权限进行监控和审计，及时发现和处理异常情况。这些措施需要综合考虑系统的实际情况和安全需求，制定出一套切实可行的账户权限管理方案。

### 3.5 用户教育与安全意识提升

(1) 网络安全知识培训。用户教育是防治网络病毒的重要一环。通过网络安全知识培训，可以提高用户的安全意识和防范能力，使用户能够更好地识别和应对网络威胁。培训内容可以包括网络安全基础知识、病毒传播方式和防范方法等方面。通过培训，可以使用户了解网络安全的重要性，掌握基本的网络安全操作技能，提高系统的整体安全性<sup>[4]</sup>。(2) 防范社交工程攻击。社交工程攻击是黑客利用人类心理和社会行为学原理来诱骗用户泄露敏感信息的一种攻击方式。为了防范社交工程攻击，需要加强用户的安全意识和防范能力。用户应该学会识别可疑的电子邮件、链接和社交媒体消息，避免点击不明链接或下载不明附件。同时，还需要保护自己的个人信息和账户密码，避免将其泄露给不信任的人或机构。

## 4 网络病毒防治技术的挑战与未来发展趋势

### 4.1 现有技术挑战

(1) 多样化的传播手段。网络病毒的传播手段日益多样化，从传统的电子邮件附件、恶意链接到利用社交工程进行钓鱼攻击，甚至通过物联网设备和云服务平台进行扩散。这些多样化的传播方式增加了病毒检测和防御的难度，使得传统的基于特征码的检测方法难以全面覆盖所有病毒变种。(2) 高技术含量的病毒攻击。随着网络技术的不断进步，病毒攻击的技术含量也在不断提高。零日攻击、勒索软件、深度伪造攻击等高技术含量的病毒不仅更难被检测和防御，而且一旦成功入侵，将给系统带来严重的破坏和数据泄露风险。(3) 不同系统安全软件的兼容性。不同操作系统和网络设备上的安全软件存在兼容性问题。这种兼容性的缺失可能导致安全漏洞的叠加和攻击面的扩大，使得防御系统更加脆弱。企业在部署安全系统时，需要花费大量时间和精力来解决不同安全工具的兼容性问题。

### 4.2 未来发展趋势

(1) 综合安全系统的创建与增强。为了应对日益复杂的网络病毒威胁，创建和增强综合安全系统将成为未来的发展趋势。这种系统将涵盖防护、检测、响应、恢复等多个环节，形成一个完整的网络安全生态系统，实现对网络威胁的全面防御。(2) 大数据与人工智能技术在病毒防治中的应用。大数据和人工智能技术在病毒防治中的应用将进一步提升防御的准确性和效率。通过大数据分析，可以实时监测网络流量和异常行为，及时发现潜在威胁。而人工智能技术则可以通过机器学习和深度学习等技术手段，自动识别和应对网络攻击，实现防御的智能化和自动化。(3) 加强政策与法律支持，提高防治效率。政府将出台更多政策和法律来支持网络病毒防治工作，明确网络安全责任和义务，加大对网络攻击行为的打击力度。这些政策和法律将为网络安全行业的发展提供有力的保障和支持，推动防治技术的不断创新和应用。(4) 开展安全技术研究和创新。为了应对不断变化的网络病毒威胁，需要持续开展安全技术研究和创新。通过研发新的安全技术和工具，不断提升防御系统的能力和效率，为网络安全提供更加坚实的保障。

### 结束语

综上所述，网络病毒防治技术在计算机管理中发挥着至关重要的作用。通过综合应用安全软件、系统更新、数据备份、网络访问控制及用户教育等多种手段，可以有效提升计算机系统的安全防护水平。未来，随着网络技术的不断进步，我们应持续关注网络病毒的新趋势，不断优化防治策略，确保计算机管理的安全性和稳定性，为数字经济的健康发展提供坚实保障。

### 参考文献

- [1]李梅.网络病毒防治技术在计算机管理中的应用分析[J].计算机产品与流通,2019,(07):80-81.
- [2]段兴林.网络环境下的计算机病毒及其防范技术[J].消费电子,2022,(06):42-44.
- [3]邵泽虎.网络病毒防治技术在计算机管理中的应用[J].电子技术与软件工程,2019,(19):189-190.
- [4]蔡志刚.计算机网络维护与病毒防治方法[J].中国高新科技,2020,(17):150-151.