网络型病毒分析与计算机网络安全技术的构建

钟百胜

（广州工商学院，广东 广州 510800）

摘　要　通过分析网络类型的病毒，运用计算机网络安全技术，可以保证网络的安全，防止网络的安全风险不断上升。尤其是随着现代资讯科技的日益普及，网络病毒层出不穷，对电脑的安全使用造成严重威胁的今天，对网络病毒及网络安全技术进行研究是十分必要的。本文将结合网络类型的病毒，对计算机网络的安全风险进行探讨，并提出相应的安全管理对策。

关键词　网络型病毒；计算机；网络安全技术

中图分类号：TP393.08　　**文献标识码**：A　　**文章编号**：1007-0745(2023)03-0019-03

在电脑技术飞速发展的今天，计算机网络给人们带来了极大的便利，同时也带来了一系列的问题，网络安全是其中一个比较严重的问题，对我们的危害很大。为了营造一个更好的网络环境，我们需要对它进行有效的防护，首先要根据它的特点建立计算机的安全技术，并采取相应的措施，这样才能营造出一个更加安全的网络环境。

1 网络型病毒概述

1.1 网络型病毒含义

网络病毒是一种典型的电脑病毒，虽然人们对它的认识逐渐提高，但对它的界定还存在着一些争议。一是计算机网络型病毒主要是通过计算机网络结构框架、网络协议体系来传播。因此，网络型病毒仅仅是局限于计算机网络范围内，攻击对象是计算机网络内部的用户；而另一种说法则更为宽泛，认为只要编写的病毒程序都可以在计算机网络上成功传播的病毒，都是属于计算机网络型病毒的。

1.2 网络型病毒特点

随着时代的发展，计算机网络技术也在飞速发展，进入了一个新的发展阶段。因为网络病毒的特殊性，它依靠电子邮件、通讯接口、网络接口等方式进行传播，与传统的磁性媒介相比，有着本质的区别。同时，针对的目标也从单一的主机向移动客户端、工作站和无线网络覆盖的所有设备延伸。随着信息化时代的到来，互联网已渗透到人们的工作、学习和生活中的每一个角落，通过一个网络端口，就可以将所有的计算机设备都感染，通过网络提供计算服务的端口和装置，使其更加扩散。所以，要完全清除这种新的网络病毒是非常困难的。这种病毒可以附着在不同的应用或者文件上，方便大规模的扩散。病毒可以通过电子邮件、电子公告板等方式传播。而随着计算机网络技术的不断进步，网络病毒也在不断地更新，特别是在自我防御、加密和追踪等技术的普及下，许多新的网络病毒变得更加隐蔽化、智能化，给计算机网络安全带来了更大的威胁。对于某些犯罪分子来说，网络病毒已成为一种以精确打击为特征的武器。网络病毒会有针对性地攻击经济、政治安全等相关信息，造成重大商业机密、国家安全等问题的发生，严重危害国家安全。

2 网络型病毒的分类

2.1 蠕虫病毒

蠕虫病毒主要是借助于MIRC以及htm文件来进行传播的，一旦使用者的电脑中了蠕虫病毒，病毒就会自动搜索本地和网络上的硬盘，找到他们的目录，搜索被感染的档案，再利用病毒代码覆盖原来的用户档案，将其修改成vbs。当计算机受到蠕虫的感染后，它的计算机资源将会被大量地消耗，从而使整个系统的运行速度大大降低。蠕虫在传播过程中，一般都是依靠宿主和网络的运转，而不是通过修改主机等文件，所以一旦蠕虫蔓延开来，很可能会让整个系统瘫痪。另外，想要查到蠕虫病毒是一件很难的事情，因为在网络上，一旦有一台电脑没有被清理掉，那么蠕虫就会重新出现。[1]

2.2 邮件病毒

邮件病毒是一种常见的病毒，它是一种以邮件的

★基金项目：2022年广州工商学院科研重点培育项目（KYPY2022044）；2021年度广州工商学院校级质量工程建设项目《基于SPOC的＜网络安全＞翻转教学实践》（ZL20211140）。

方式传播的病毒，因为它是一种很好的通讯工具，所以会被互联网用户广泛使用，比如有很多用户使用邮件发布求职信等，这就导致邮件病毒有了可乘之机。这种病毒是微软 outlook 客户机的一种特性，它可以让使用者在收到邮件后，在病毒的驱动下，将带有病毒的电子邮件传送到通讯录上的使用者。

2.3 马丁病毒

马丁是一个包含客户机和伺服器的后门程式，通常被用作黑客工具。马丁病毒能够截获使用者的信息，而不需要使用者自己去做，虽然没有任何的复制能力，但是一旦使用者使用，就会控制住电脑，对使用者造成巨大的伤害。

2.4 木马病毒

木马病毒包括服务器和客户机，它是一种后台软件。通常，木马是黑客利用的入侵、攻击手段，在使用者毫无察觉的情况下窃取、篡改重要资料。就算木马病毒本身不能自己复制，但一旦使用者的电脑安装了木马，那么它就会被入侵，这就造成了很大的危害，所以一般都是在电脑里安装木马，让使用者误以为它是病毒。

2.5 复合型病毒

复合病毒是由多个不同的病毒组合而成，有可能是导入区，也有可能是某个文件，如果不能将其完全消灭，那么它的复活概率就会大大增加。可以说，这种病毒的处理是一件很困难的事情，也就是说，要想将这些复杂的病毒全部清除，必须要有一个文件和一个向导。

3 防范网络型病毒的计算机网络安全技术

3.1 数据加密网络安全技术

分析数据本身的网络加密技术，并依据数据加密技术的特点，在实际应用中也能保持网络的安全性。在传输过程中加入一些合理的算法，保证数据的融合，并保证数据的正确使用。在这种方式下，数据会被加密，不能被非法的使用者看到，采用两种数据保护机制来保证系统的安全。另外，采用一种全新的计算机协议，对计算机的密码方式进行全面的逻辑分析，通常加密包括节点加密、端口加密等。另外，在密码管理方面，可以使得整个数据的传送和存储更为完美。在此基础上，采用计算机虚拟安全技术，以整个密码系统为核心，保证用户在私有局域网中可以进行网络业务的连接。引进集中式网络技术，让它建立起一个共同的网络。并且，该网络还可以根据虚拟网络开发出一个新的结点，并根据端口的链接，将公用的网络资源组合在一起。从现实的角度对计算机虚拟中心网技术进行分析，并对其进行技术验证。其中，身份认证、密码技术认证、隧道认证等都是为了保证网络信息的安全性，同时也是为了保证网络的安全。同时，保证系统的可操作性和有效性。在计算机上使用虚拟网络的安全技术是提高计算机自身安全水平的关键。

3.2 入侵检测网络安全技术

入侵检测是一种针对网络病毒的入侵，防止被盗取和篡改的系统。基于 IDS，可以快速地识别、分析网络的信息，或者在主机上进行分析，然后由中央控制台进行监控和管理。其实，IDS 是一种比较典型的窃听器，它不会连接到多个物理层，只有一个监听口，可以在没有流量的情况下悄无声息地在网络上收集报文。入侵检测能够迅速地发现异常，结合正常情况下的进程特征和用户特征，建立相应的模型，并将其与正常的行为模式进行对比分析，如果有很大的偏差，就是异常。这种技术可以让使用者在不需要知道攻击的特性的情况下，就能侦测到敌人的攻击，并根据使用者的动作进行更新。误用检测是将攻击特征与特征库中的攻击特征进行比较，从而判断是否存在入侵。该技术具有很高的准确率，能够识别多种攻击，并在最短的时间内阻止攻击。但这种技术有一个弊端，那就是在新的攻击下，它不能检测到任何攻击，所以必须不断地更新攻击记录，以防止攻击。[2]

3.3 防火墙网络安全

防火墙技术是计算机网络安全的典型代表，它的作用是将危险区域与安全区域分离，提高网络的安全性。防火墙是一种具有很好的防毒性能的网络过滤系统，它根据使用者设定的安全标准，对进入和离开的网络进行过滤，并对病毒进行有效的防御，防止病毒进入电脑的端口。随着防火墙技术的发展，技术的进步越来越快，越来越普及。防火墙技术是以网络为基础对特定的地址和服务进行过滤，并对所传送的数据源进行必要的检测，以确保数据包的通讯速度，并对常用的病毒载体进行扫描和清除。这样，网络的抗性就会大大提高。可以设定不同的防火墙，并且针对高级的安全，会禁止一些像视频流这样的服务。当前的防火墙体系结构采用粗糙的存取方式，将内部网络作为一个逻辑单位来进行处理。但是，这种访问控制器系统不能满足高级别的计算机网络的安全保护需求。在应用防火墙技术时，应着重于其功能的发挥。从实践上讲，防火墙并不能阻止病毒的入侵，并且在不同的防火墙间进行数据的更新是一项技术难点，最大的延迟会导致服务器的实时存取要求不能及时响应。所以，防火墙是一种融合了各种尖端技术的复合型技术，并不是单纯地将病毒与外界隔离开来。[3]

3.4 计算机虚拟专用网络安全技术

虚拟专用网主要采用公用数据网，并以此为前提，确保用户可以直接利用私有局域网进行联网。计算机虚拟私有网络的安全技术的基本要求是由提供网络的提供者和提供商利用公共网络来建立的。在这种特殊的虚拟网中，由于存在着两个不同的结点，因此无需利用传统的端口与端口间的链接，能够充分地利用现有的公共网络资源的高效构成和使用。根据现实情况，电脑虚拟专用网络安全技术主要用于个人资料的传送。在这些技术中，应用最多的是身份认证、隧道技术、加密解密技术以及密钥管理技术。利用这些技术，可以提高网络信息的安全性，降低某些未知信息的拦截、窃听、信息篡改等，从而提高了整个网络的安全性。尤其是在网络的整体设计过程中，网络的整体结构更为简洁，随着网络的安全性不断提高，其可扩展性也会越来越大。目前，计算机虚拟专用网络安全技术已成为计算机网络安全技术的重要内容。

4 计算机网络安全技术的构建

4.1 安装杀毒软件

为了防止网络病毒的侵入，用户应该在使用计算机之前安装防病毒软件，并定期进行杀毒，以便能够及时发现并清除可能存在的病毒，并及时清除，既保证了电脑的安全，又避免了系统的瘫痪。通过安装防病毒软件，对计算机的网络进行实时监控，并对关键文档采取个性化的保护措施，实现了对重要文档的保护。此外，需要定期进行补丁的更新，以及时修补电脑的漏洞，尽量降低电脑病毒的入侵概率，提高电脑的安全性。[4]

4.2 及时更新网络系统的补丁

及时更新系统的补丁，可以增强系统的稳定性。许多病毒都是由于系统故障才会被感染或者被攻击。因此，为了保证操作系统的整体安全，应及时进行系统补丁。每个星期都要进行一次升级，并且在安装完毕之后重新启动。另外，为了防止恶意软件和恶意软件的入侵，必须要关机。

4.3 提高计算机人员的综合素质能力

IT 产业的特殊性和广泛的应用范围，使得它在网络环境中发挥了很好的作用。不过，IT 病毒也可以制造出类似于网络病毒的病毒，根据资料显示，大部分的病毒制造者都是 IT 从业人员，他们拥有强大的技术和较低的专业技能，使得网络病毒数量不断增长。所以，强化 IT 员工的职业素养是很有必要的。IT 从业人员既要做好自己的工作，又要严格要求自己，规范自己的网络行为，从而推动我国计算机产业的发展。

4.4 采用个性化的网络病毒预防措施

网络病毒有广泛性，所以病毒可以利用这种特性进行大规模的扩散，通过对文件和源代码进行特殊的设定，从而达到高效的传播效果。通过灵活地修改文件和源代码，但病毒不会因为文化和源代码而改变。该方法通过扩展文件名称和修改的方式实现子档的加密，使关联不能找到攻击目标，提高了文件和源代码的安全。

4.5 建立计算机网络安全监督管理系统

相关部门需要加大力度进行监督，促使责任制更加完善，在对计算机网络和信息安全应用以及管理中，本着认真负责的态度，将预防作为重点予以综合性治理。同时，还实现了人员和技术的结合。通过对安全保护责任制的制定，构建完善制度或者增加数据保密与动态口令认证系统的安装都十分重要。信息安全的另一种形式为数据保密，也就是利用的密码技术，在各个领域发展中，随着计算机网络的广泛利用，密码学也得到扩大，比如，使用的数字签名、身份鉴别等都是从密码学技术衍生的一种技术。网络安全也不例外，由于网络使用的简单易行和其特有的开放性以及应用环境的多样化等因素，使得计算机网络信息的安全和保密问题变得越来越重要，网络安全技术作为一个独特的领域受到越来越多的关注。[5]

5 结语

综上所述，网络病毒具有极强的传染性和破坏性，一旦被感染就会迅速扩散，严重的话会造成系统的瘫痪、数据丢失、篡改。因此，在了解网络类型病毒特点的前提下，寻找一种合理、可靠的计算机网络防御技术，对计算机的计算和操作进行实时监控，从而实现对病毒的有效追杀。

参考文献：

[1] 马斐 . 网络型病毒分析与计算机网络安全技术构建 [J]. 科技资讯 ,2022,20(24):26-29.
[2] 翟哲 . 网络型病毒分析与计算机网络安全技术研究 [J]. 电子技术与软件工程 ,2021(23):256-257.
[3] 黄作鹏 , 岳佳欣 . 网络型病毒分析与计算机网络安全技术研究 [J]. 电子技术与软件工程 ,2021(09):255-256.
[4] 徐文超 . 网络型病毒分析与计算机网络安全技术构建 [J]. 科技资讯 ,2019,17(27):16,18.
[5] 王枫 . 网络型病毒分析与计算机网络安全技术构建 [J]. 信息通信 ,2018(01):141-143.