ISSN:2705-0963（Print）　ISSN:2705-0955（Online）

浅谈计算机病毒原理与防范

黄　鑫

黑龙江财经学院　黑龙江　哈尔滨　150000

摘　要：近年来计算机技术发展速度很快，并逐步渗透到社会的各个方面，也推动了社会生产力的提升，但是网络病毒是当下网络安全防范的重点与难点。网络是一个硬件与软件兼具的系统，其是以虚拟的形式存在的，在网络环境下，用户能够用网络连接的方式获得足够的资料与想要的数据。借助网络平台，人们可以实现利益与信息的双重收获，但是其安全隐患是十分明显的，网络平台极容易受到病毒的供给，用户的信息也会得到不同程度的泄露，其基本权益也受到了严重的威胁。因此，本文分析了计算机病毒原理与防范的措施，以供广大相关人士参考。

关键词：计算机；病毒；防范措施

随着科技水平不断进步，计算机的应用渗入到了社会生活的方方面面。随之而来的计算机病毒依靠其传染性、隐蔽性和破坏性等特点，对计算机系统及其应用程序造成潜在风险和重大损害。当今社会对计算机依赖程度越来越高，计算机安全也受到了更多的关注，文章对计算机病毒原理与防范的措施进行了分析和研究。

一、计算机病毒类型

计算机病毒入侵是一个多义词，是指计算机系统通过各种途径被病毒传染，它主要用于植入病毒窃取用户数据资料、攻击计算机系统等，病毒入侵一旦发生，将导致计算机各种性能下降或运行不稳定，以至于无法进行正常操作，严重时计算机系统将瘫痪。计算机病毒的入侵大致分为 4 种类型：（1）源代码嵌入攻击型。该型病毒主要是对语言的源程序进行入侵，其将病毒代码在源程序编译完成之前插入，这就导致新生成的可执行文件附带了病毒代码，变成了一个新的病毒传播源。鉴于在源程序里插入病毒代码要求的专业水平较高，以及获取各类软件编译前的源程序有一定的难度，所以此类可执行病毒文件较少出现。（2）外壳附加型。大多数文件型的病毒属于外壳附加型，这种类型的病毒一般是将其病毒代码嵌入到程序的正常代码内，类似于给程序套上了一个外壳，在使用者执行被嵌入了病毒代码的程序时，病毒代码将在正常程序被调入内部存储器前先行执行。（3）系统修改型。这类病毒主要攻击操作系统，它用自身的程序文件替换或篡改系统中的相应文件，以此来达到替换或执行操作系统中部分应用的目的，此类病毒是一种常见的类型，多表现为文件型病毒，感染破坏操作系统，危害性大。（4）代码取代攻击性。该类计算机病毒主要是用病毒代码覆盖相应被入侵程序的整个或部分代码，这类病毒也少见，它主要作用于特定的程序，隐蔽性高、针对性强，不易清除。

二、网络型病毒概述

计算机在实际使用过程中，计算机病毒的产生会对其造成更大危害，尤其是人为编码形成的代码或者是程序。在当今社会发展下，计算机病毒的种类更加多样，如；基于寄生对象的划分，主要是混合型的病毒、文件型的病毒以及引导型的病毒等。基于特有算法进行划分、按照危害的程度或者结合链条形式的划分等有不同类型。对于网络型病毒的特点，其具备较强的隐蔽性和破坏性，具备的传播形式更复杂，其传播范围广。不仅如此，传播的速度也更快，无法简单对其清除。基于相关资料信息的统计，发现目前为止，已经有 86% 以上的网络型病毒，在对其清除后，发现一个月以内还会再一次感染。计算机病毒是在对计算机程序进行编制或者实施插入的时候，将计算机的功能以及数据带来明显的破坏性，影响计算机的使用，能够在期间对计算机的指令或者程序代码进行复制，具备明显的破坏性和传染性。一般情况下，病毒主要潜伏在计算机的内部储存中，如果外部条件符合的时候就会被激活，能将自身复制到其他的程序中，给其他文件带来一定的感染性，从而给计算机资源带来更为严重的破坏性。从当前实际情况看，计算机病毒的分类是按照感染对象划分的，分别为文件病毒、复合型病毒以及引导型病毒和网络型病毒。在这些类型中，传播最快的则为网络型病毒。近几年网络型病毒在互联网领域高速发展，且网络型病毒感染的对象和攻击方式、传播方式也从单一的方式逐渐复杂化，隐蔽性极强。比如；以前感染的文件只有 Word 文档和 Excel 表格、电子邮件等，现在，则会将所有的 office 文件感染，不仅能对文件进行修改和删除，也将发生文档内容的盗取、加密等情况，且感染传播的方式也从原来的磁盘工具转变为网络化传播。

三、网络病毒的危害

由于网络病毒传播速度快、范围广且难以有效清除，使得计算机一旦感染上网络病毒，就会影响到设备的正常使用，而且用户的资料、数据等资源也会遭到破坏，给用户造成极大的损失。比如木马病毒，在入侵计算机后在操作系统中潜伏，然后盗取用户的 QQ 密码、银行密码等信息。还有蠕虫病毒，相比于木马病毒来讲更加先进，它的传播途径十分广泛，危害也更大。这是因为蠕虫病毒可以主动扫描计算机的漏洞，并对这些漏洞发起进攻，在感染一台计算机后，蠕虫病毒通过网络迅速扩充感染范围，并发送大量数据包占据网络带宽，而主机内存的占用也会变得过高，最终导致死机。可以说网络病毒是计算机管理中的一大难点，特别是在各大高校的计算机实验室，计算机被感染的风险更大。如果其中一台计算机感染，那么计算机操作系统将会出现各种异常，不仅影响相关课程实验的正常开展，还给计算机管理人员增加工作负担。而对于各大企业来说，一旦计算机感染上网络病毒，就不止意味着工作效率会降低，还很有可能面临数据被窃取、篡改等风险，给企业的正常运行带来极大的阻力。网络病毒不仅威胁着计算机中的各种资源，还会让网络系统面临崩溃的风险，给人们的正常生活带来阻碍，所以不管从什么方面去考虑，它的危害都是极大的。

四、计算机病毒的防范措施

（一）树立计算机病毒防范意识

重视计算机病毒可能给计算机安全带来的危害，养成良好的计算机操作习惯，不运行和打开来历不明的程序、电子邮件，不访问非法、山寨网站，定期对计算机内重要数据和文件进行异地备份。掌握一些必要的计算机病毒防范知识，

ISSN:2705-0963（Print） ISSN:2705-0955（Online）

以减少病毒可能对计算机系统造成的损害。

（二）发现及清除计算机病毒

面对层出不穷的新病毒和变种病毒，安装正版杀毒软件和防火墙等防御性软件就显得十分必要。要及时升级杀毒软件病毒库和扫描引擎，使其保持在最新的状态，以便能及时隔离、查杀新病毒和变种病毒。定期或设置按时自动扫描计算机，能保障计算机系统的健康运行并及时清除病毒。

（三）阻断感染计算机病毒的途径

通过了解计算机病毒常见的入侵和传播途径，可以在很大程度上减小计算机感染病毒的几率。联网计算机不要在不了解的网站下载运行应用程序，不要随意打开微信、QQ 等聊天工具或论坛上的未知链接。设置网络接入和计算机登录密码时，应在区分大小写的同时，充分运用包含符号、字母、数字的组合性密码，避免使用过于简单的密码组合，以提高网络和系统的密码安全性。不要随意启用计算机的共享功能，日常在使用光盘、优盘等安装应用程序和拷贝文件时，应先使用杀毒软件进行扫描，防止带毒文件通过存储介质感染计算机。

（四）利用网络病毒检测技术，加强计算机安全管理

在计算机网络病毒防治工作中，病毒检测是首要工作，也是重要工作，只有及时检测到病毒，才能防止病毒对计算机造成危害。目前的网络病毒检测技术较多，这里以文件校验技术为例，介绍其在计算机管理中的应用。文件校验技术是利用病毒很难以独立的形式存在，需要依附在一定的载体上这一特性，对网络病毒进行检测。当病毒入侵到计算机中的文件时，文件的大小、修改日期等都会发生变化。计算机管理人员在日常管理工作中可以对计算机的运行情况进行观察，比如当计算机出现 CPU 占用突然增大、有明显卡顿等情况时，可以初步判定计算机受到了网络病毒的感染。然后管理人员可以在病毒查杀软件的辅助下对系统中的文件进行安全校验，对计算机已经感染病毒的状况进行更加精准地检测和判定。但是这种检测方式还是不够全面，虽然能很好地检测到网络病毒，但是无法对病毒的具体情况展开分析以给出清除病毒的意见。

（五）使用病毒防御技术，提高计算机安全性

能防御是计算机网络病毒防治的根本，随着病毒入侵技术的不断进步，想要精确地检测网络病毒并将之清除是十分困难的，而且需要花费的时间和经济成本也比较高。所以，在计算机管理工作中，为了提高计算机的安全性能，还应该将工作重心放在计算机网络病毒的防御中。当前，主要的病毒防御技术有单机防御技术、机组防御技术、联动防御技术、数据挖掘防御技术等。其中联动防御技术使用较多，该技术与防火墙技术有着紧密地联系，该技术能基于网络安全策略检测网络中的异常情况，并将异常信息发送到计算机的防火墙，让防火墙对这些异常进行拦截、抵御处理。最后及时将病毒的信息和判定结果反馈给网关，网关在收到信息警示后发起隔离控制，使网络病毒被隔断在网关外。这种防御技术在控制病毒传播上有着非常明显的效果，因此也被很好地推广应用在计算机管理中，管理人员只需安装好防火墙，系统就可以为计算机开启防御模式，让不符合要求的访问者隔离在外部网络中，很好地抵御病毒的入侵。

（六）使用备份技术，保障数据安全数据

安全是计算机管理工作的一大难点，在数据时代，这些数据信息不仅意味着财富，还有用户的信息安全。一旦网络病毒入侵到用户的计算机，很多重要数据可能会丢失，所以为了降低病毒的破坏，备份技术的应用是很有必要的。目前常见的数据备份策略有完全、差分和增量备份三种。其中完全备份是指在某一时间点上，对系统的所有数据进行备份。这种备份方式的优势在于，能够在数据丢失时快速恢复数据，但是对存储空间提出了更高的要求。而增量备份是在第一次完全备份的基础上，记录每次重新备份时发生变化的数据。以增加恢复数据的时间为代价，换取存储空间的减少，当然，在使用该技术进行数据备份时速度更快。差异备份则是在第一次完全备份的基础上，记录最新一次备份数据的第一次备份数据的差异，这种备份技术考虑了前两种备份技术的缺点，计算机用户只需两次备份数据就既能完全恢复数据，又不必占用过多的存储空间。

（七）使用杀毒技术，定期查杀病毒

一方面，计算机系统中的漏洞是难以避免的，另一方面，寻找漏洞也需要花费大量的时间，如果在修复漏洞之前，网络病毒对这些漏洞展开攻击，就可能使计算机受到入侵。因此计算机管理人员在对系统的漏洞进行修复的同时，还要应用好各种病毒防御技术，完善计算机系统的安全性能。计算机管理人员可以使用杀毒技术对病毒进行全面查杀，如果软件提示系统存在网络漏洞，计算机管理人员就需要及时为漏洞打上补丁，防止网络病毒的攻击，维持计算机的正常运行。为了能够实现杀毒软件对计算机的持续保护，在计算机管理中最好对杀毒软件进行及时升级，以保证杀毒技术能够随之更新，充分发挥杀毒软件的作用。

（八）加强内部管理

内部管理的加强主要是从以下几方面入手，首先就是对所有的主机与设备都进行加密处理，所使用的密码要足够长、复杂，并且还不能被随意破解，要及时作出更换。其次需要严格控制各项设备的访问权限，并保证权限密码的多样性，尽量要尽可能少的人知道，一般的成员只能登陆设备使用。对访问权限进行控制不仅仅是为了保护设备更是为了保护计算机的权限、操作与配置等。

（九）完善管理制度

要结合计算机网络具体运行状况，不断对相关管理制度进行完善，让网络设备始终处于安全环境中运行，避免出现网络安全问题。对服务器、主干交换机等设备来说，应该将管理措施做到位，所有通信线路必须做出架空、深埋与穿线处理，将相关标识做好，同时各终端设备要采取有效管理方法。要结合我国现行法律法规，严格落实信息安全管理制度，将各人员的具体职责明确下来，让用户个人信息得到安全保护。管理人员应该增强安全意识，加强对他们的安全技术培训，能够主动将应急保护工作提前做好，及时更换故障设备，确保计算机正常运行。

五、结语

综上所述，计算机病毒在很大程度上影响着现代人们的生活与工作，其能够通过各种形式大范围快速传播，严重威胁着计算机信息安全。对此我们应该提前做好防范措施，最大限度消除计算机网络病毒带来的危害，这样才能最大限度地保证网络安全的清净。

参考文献：

［1］史智恒 . 计算机系统安全与计算机网络安全研究［J］. 信息通信，2019（5）:189-190.

［2］张伟 . 计算机应用教学的研究现状［J］. 信息化建设，2020（1）:104.

［3］韩勇 . 计算机病毒防治方法的探讨［J］. 信息与电脑，2020（4）:166-167.

［4］王海飞 . 计算机病毒及其防治策略［J］. 信息与电脑（理论版），2020（3）:193-195.

［5］姜学东，王昊欣 . 计算机病毒与防范对策研究［J］. 无线互联科技，2020（9）:31-32.