摘　要

随着计算机网络技术的快速发展，网络安全日益成为人们的焦点，计算机病毒作为计算机安全的主要威胁，正在受到人们广泛的关注。因为在网络上，面临名目繁多的计算机病毒威胁计算机病毒将导致计算机系统瘫痪，程序和数据严重破坏，使网络的效率和作用大大降低，使许多功能无法使用或不敢使用。层出不穷的各种各样的计算机病毒活跃在各个网络的每个角落，如近几年的“冲击波”、“震荡波”、“熊猫烧香病毒”给我们的正常工作已经造成过严重威胁。下面就计算机网络存在的安全隐患及相关策略进行探讨分析。

关键字：**网络安全　、病毒**

Abstract

With the computer network technology has developed rapidly, the network security is to be the focus of the computer virus computer security, as the major threats are attracted wide attention. because the internet, the face of various kinds of computer viruses threat to the computer virus will lead to a computer system paralysis, procedures and data serious damage to network efficiency and reduced significantly, many function was unable to use or not to use. Endless variety of computer virus active in the network every nook and cranny of the past few years, such as "the dreaded combusted blast wave", "shock wave", "panda and viruses to our work has been a serious threat. the following is the existence of a computer network to explore and related policy analysis.

Keyword : network security : virus

计算机网络安全策略浅议

一、计算机网络存在的病毒威胁分析

近年来随着 Internet 的飞速发展，计算机资源的损失和破坏，不但会造成资源和财富的巨大浪费，而且有可能造成社会性的灾难，随着信息化社会的发展，计算机病毒的威胁日益严重，反病毒的任务也更加艰巨了。1988 年 11 月 2 日下午 5 时 1 分 59 秒，美国康奈尔大学的计算机科学系研究生，23 岁的莫里斯（Morris）将其编写的蠕虫程序输入计算机网络，致使这个拥有数万台计算机的网络被堵塞。这件事就像是计算机界的一次大地震，引起了巨大反响，震惊全世界，引起了人们对计算机病毒的恐慌，也使更多的计算机专家重视和致力于计算机病毒研究

1.1 病毒的定义、分类

计算机病毒(Computer Virus)在

《中华人民共和国计算机信息系统安全保护条例》中被明确定义，病毒指“编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自 我复制的一组计算机指令或者程序代码”。而在一般教科书及通用资料中被定义为:利用计算机软件与硬件的缺陷，由被感染机内部发出的破坏计算机数据并影响计算机正常工作的一组指令集或程序代码 。计算机病毒最早出现在70年代 David Gerrold 科幻小说 *When H.A.R.L.I.E. was One*.最早科学定义出现在1983:在 Fred Cohen (南加大) 的博士论文 “计算机病毒实验” “一种能把自己(或经演变)注入其它程序的计算机程序 ”启动区病毒,宏(macro)病毒,脚本(script)病毒也是相同概念传播机制同生物病毒类似 .生物病毒是把自己注入细胞之中。

1.1.(1)系统病毒

系统病毒的前缀为：Win32、PE、Win95、W32、W95等。这些病毒的一般共有的特性是可以感染 windows 操作系统的 *.exe 和 *.dll 文件，并通过这些文件进行传播。如 CIH 病毒。

1.1.(2)蠕虫病毒

蠕虫病毒的前缀是： Worm 。这种病毒的共有特性是通过网络或者系统漏洞进行传播，很大部分的蠕虫病毒都有向外发送带毒邮件，阻塞网络的特性。比如冲击波（阻塞网络），小邮差（发带毒邮件） 等。

1.1.(3)木马病毒、黑客病毒

木马病毒其前缀是：Trojan，黑客病毒前缀名一般为 Hack 。木马病毒的共有特性是通过网络或者系统漏洞进入用户的系统并隐藏，然后向外界泄露用户的信息，而黑客病毒则有一个可视的界面，能对用户的电脑进行远程控制。木马、黑客病毒往往是成对出现的，即木马病毒负责侵入用户的电脑，而黑客病毒则会通过该木马病毒来进行控制。现在这两种类型都越来越趋向于整合了。一般的木马如 QQ 消息尾巴木马 Trojan.QQ3344 ，还有大家可能遇见比较多的针对网络游戏的木马病毒如 Trojan.LMir.PSW.60 。这里补充一点，病毒名中有 PSW 或者什么 PWD 之类的一般都表示这个病毒有盗取密码的功能（这些字母一般都为“密码”的英文“password”的缩写）一些黑客程序如：网络枭雄（Hack.Nether.Client）等。

1.1.(4)脚本病毒

脚本病毒的前缀是： Script 。脚本病毒的共有特性是使用脚本语言编写，通过网页进行的传播的病毒，如红色代码（Script.Redlof）。脚本病毒还会有如下前缀：VBS 、JS（表明是何种脚本编写的），如欢乐时光（VBS.Happytime）、十四日（Js.Fortnight.c.s）等。

1.1.(5)宏病毒

其实宏病毒是也是脚本病毒的一种，由于它的特殊性，因此在这里单独算成一类。宏病毒的前缀是：Macro，第二前缀是：Word 、Word97 、Excel 、Excel97（也许还有别的）其中之一 。凡是只感

染 WORD97及以前版本 WORD 文档的病毒采用 Word97做为第二前缀，格式是： Macro.Word97；凡是只感染 WORD97以后版本 WORD 文档的病毒采用 Word 做为第二前缀，格式是： Macro.Word；凡是只感染 EXCEL97及以前版本 EXCEL 文档的病毒采用 Excel97做为第二前缀，格式是：

Macro.Excel97；凡是只感染 EXCEL97以后版本 EXCEL 文档的病毒采用 Excel 做为第二前缀，格式是： Macro.Excel，以此类推。该类病毒的共有特性是能感染 OFFICE 系列文档，然后通过 OFFICE 通用模板进行传播，如：著名的美丽莎（Macro.Melissa）。

1.1.(6)后门病毒

后门病毒的前缀是： Backdoor 。该类病毒的共有特性是通过网络传播，给系统开后门，给用户电脑带来安全隐患。

1.1.(7)病毒种植程序病毒

这类病毒的共有特性是运行时会从体内释放出一个或几个新的病毒到系统目录下，由释放出来的新病毒产生破坏。如：冰河播种者（Dropper.BingHe2.2C）、MSN 射手（Dropper.Worm.Smibag）等。

1.1.(8)破坏性程序病毒

破坏性程序病毒的前缀是： Harm 。这类病毒的共有特性是本身具有好看的图标来诱惑用户点击，当用户点击这类病毒时，病毒便会直接对用户计算机产生破坏。如：格式化 C 盘（Harm.formatC.f）、杀手命令（Harm.Command.Killer）等。

1.1.(9)玩笑病毒

玩笑病毒的前缀是：Joke 。也称恶作剧病毒。这类病毒的共有特性是本身具有好看的图标来

诱惑用户点击，当用户点击这类病毒时，病毒会做出各种破坏操作来吓唬用户，其实病毒并没有对用户电脑进行任何破坏。如：女鬼（Joke.Girl ghost）病毒。

1.1.(10)捆绑机病毒

捆绑机病毒的前缀是：Binder。这类病毒的共有特性是病毒作者会使用特定的捆绑程序将病毒与一些应用程序如 QQ、IE 捆绑起来，表面上看是一个正常的文件，当用户运行这些捆绑病毒时，会表面上运行这些应用程序，然后隐藏运行捆绑在一起的病毒，从而给用户造成危害。如：捆绑 QQ（Binder.QQPass.QQBin）、系统杀手（Binder.killsys）等。以上为比较常见的病毒前缀，有时候我们还会看到一些其他的，但比较少见，这里简单提一下：DoS：会针对某台主机或者服务器进行 DoS 攻击；Exploit：会自动通过溢出对方或者自己的系统漏洞来传播自身，或者他本身就是一个用于 Hacking 的溢出工具；HackTool：黑客工具，也许本身并不破坏你的机子，但是会被别人加以利用来用你做替身去破坏别人。你可以在查出某个病毒以后通过以上所说的方法来初步判断所中病毒的基本情况，达到知己知彼的效果。在杀毒无法自动查杀，打算采用手工方式的时候这些信息会给你很大的帮助。

1.2 病毒的产生

病毒不是来源于突发或偶然的原因。一次突发的停电和偶然的错误，会在计算机的磁盘和内存中产生一些乱码和随机指令，但这些代码是无序和混乱的，病毒则是一种比较完美的，精巧严谨的代码，按照严格的秩序组织起来，与所在的系统网络环境相适应和配合起来，病毒不会通过偶然形成，并且需要有一定的长度，这个基本的长度从概率上来讲是不可能通过随机代码产生的。现在流行的病毒是由人为故意编写的，多数病毒可以找到作者和产地信息，从大量的统计分析来看，病毒作者主要情况和目的是：一些天才的程序员为了表现自己和证明自己的能力，出于

对上司的不满，为了好奇，为了报复，为了祝贺和求爱，为了得到控制口令，为了软件拿不到报酬预留的陷阱等．当然也有因政治，军事，宗教，民族．专利等方面的需求而专门编写的，其中也包括一些病毒研究机构和黑客的测试病毒．

1.3 病毒的攻击发展过程

在病毒的发展史上，病毒的出现是有规律的，一般情况下一种新的病毒技术出现后，病毒迅速发展，接着反病毒技术的发展会抑制其流传。操作系统升级后，病毒也会调整为新的方式，产生新的病毒技术。它可划分为：

1.3(1) DOS 引导阶段

1987 年，计算机病毒主要是引导型病毒，具有代表性的是“小球”和“石头”病毒。当时的计算机硬件较少,功能简单,一般需要通过软盘启动后使用.引导型病毒利用软盘的启动原理工作,它们修改系统启动扇区,在计算机启动时首先取得控制权,减少系统内存,修改磁盘读写中断,影响系统工作效率,在系统存取磁盘时进行传播； 1989 年,引导型病毒发展为可以感染硬盘,典型的代表有“石头 2”；

1.3(2) DOS 可执行阶段

1989 年,可执行文件型病毒出现,它们利用 DOS 系统加载执行文件的机制工作,代表为“耶路撒冷”，“星期天”病毒,病毒代码在系统执行文件时取得控制权,修改 DOS 中断,在系统调用时进行传染,并将自己附加在可执行文件中,使文件长度增加。 1990 年,发展为复合型病毒,可感染 COM 和 EXE 文件。

1.3.(3) 伴随、批次型阶段

1992 年,伴随型病毒出现,它们利用 DOS 加载文件的优先顺序进行工作，具有代表性的是“金

蝉”病毒,它感染 EXE 文件时生成一个和 EXE 同名但扩展名为 COM 的伴随体；它感染文件时,改原来的 COM 文件为同名的 EXE 文件,再产生一个原名的伴随体,文件扩展名为 COM，这样,在 DOS 加载文件时,病毒就取得控制权.这类病毒的特点是不改变原来的文件内容,日期及属性,解除病毒时只要将其伴随体删除即可。在非 DOS 操作系统中,一些伴随型病毒利用操作系统的描述语言进行工作,具有典型代表的是“海盗旗”病毒,它在得到执行时,询问用户名称和口令,然后返回一个出错信息,将自身删除。批次型病毒是工作在 DOS 下的和“海盗旗”病毒类似的一类病毒。

1.3.(4) 幽灵、多形阶段

1994 年,随着汇编语言的发展,实现同一功能可以用不同的方式进行完成,这些方式的组合使一段看似随机的代码产生相同的运算结果。幽灵病毒就是利用这个特点,每感染一次就产生不同的代码。例如“一半”病毒就是产生一段有上亿种可能的解码运算程序,病毒体被隐藏在解码前的数据中,查解这类病毒就必须能对这段数据进行解码,加大了查毒的难度。多形型病毒是一种综合性病毒,它既能感染引导区又能感染程序区,多数具有解码算法,一种病毒往往要两段以上的子程序方能解除。

1.3.(5) 生成器,变体机阶段

1995 年,在汇编语言中,一些数据的运算放在不同的通用寄存器中,可运算出同样的结果,随机的插入一些空操作和无关指令,也不影响运算的结果,这样,一段解码算法就可以由生成器生成，当生成器的生成结果为病毒时,就产生了这种复杂的“病毒生成器” ，而变体机就是增加解码复杂程度的指令生成机制。这一阶段的典型代表是“病毒制造机” VCL,它可以在瞬间制造出成千上万种不同的病毒,查解时就不能使用传统的特征识别法,需要在宏观上分析指令,解码后查解病毒。

1.3.(6) 网络,蠕虫阶段

1995 年,随着网络的普及,病毒开始利用网络进行传播,它们只是以上几代病毒的改进.在非 DOS 操作系统中,“蠕虫”是典型的代表,它不占用除内存以外的任何资源,不修改磁盘文件,利用网络功能搜索网络地址,将自身向下一地址进行传播，有时也在网络服务器和启动文件中存在。

1.3.(7) 视窗阶段

1996 年,随着 Windows 和 Windows95 的日益普及,利用 Windows 进行工作的病毒开始发展,它们修改(NE,PE)文件,典型的代表是 DS.3873,这类病毒的机制更为复杂,它们利用保护模式和 API 调用接口工作,解除方法也比较复杂。 宏病毒阶段 1996 年,随着 Windows Word 功能的增强,使用 Word 宏语言也可以编制病毒,这种病毒使用类 Basic 语言、编写容易、感染 Word 文档等文件，在 Excel 和 AmiPro 出现的相同工作机制的病毒也归为此类，由于 Word 文档格式没有公开，这类病毒查解比较困难。

1.3(8) 互连网阶段

1997 年,随着因特网的发展,各种病毒也开始利用因特网进行传播,一些携带病毒的数据包和邮件越来越多,如果不小心打开了这些邮件,机器就有可能中毒；

1.3(9) 邮件炸弹阶段

1997 年,随着万维网（Wold Wide Web）上 Java 的普及,利用 Java 语言进行传播和资料获取的病毒开始出现,典型的代表是 JavaSnake 病毒，还有一些利用邮件服务器进行传播和破坏的病毒，例如 Mail-Bomb 病毒，它会严重影响因特网的效率。

1.4 计算机病毒攻击事件

1.4.(1) Elk Cloner（1982年）

它被看作攻击个人计算机的第一款全球病毒，也是所有令人头痛的安全问题先驱者。它通过苹果 Apple II 软盘进行传播。这个病毒被放在一个游戏磁盘上，可以被使用 49 次。在第 50 次使用的时候，它并不运行游戏，取而代之的是打开一个空白屏幕，并显示一首短诗。

1.4.(2) Brain（1986年）

Brain 是第一款攻击运行微软的受欢迎的操作系统 DOS 的病毒，可以感染感染 360K 软盘的病毒，该病毒会填充满软盘上未用的空间，而导致它不能再被使用。

1.4.(3) Morris（1988年）

Morris 该病毒程序利用了系统存在的弱点进行入侵，Morris 设计的最初的目的并不是搞破坏，而是用来测量网络的大小。但是，由于程序的循环没有处理好，计算机会不停地执行、复制 Morris ，最终导致死机。

1.4.(4) CIH（1998年）

CIH 病毒是迄今为止破坏性最严重的病毒，也是世界上首例破坏硬件的病毒。它发作时不仅破坏硬盘的引导区和分区表，而且破坏计算机系统 BIOS，导致主板损坏。 此病毒是由台湾大学生陈盈豪研制的，据说他研制此病毒的目的是纪念 1986 年的灾难或是让反病毒软件难堪。

1.4.(5) Melissa（1999年）

Melissa 是最早通过电子邮件传播的病毒之一，当用户打开一封电子邮件的附件，病毒会自动发送

到用户通讯簿中的前 50 个地址，因此这个病毒在数小时之内传遍全球。

1.4.(6) Love bug（2000年）

Love bug 也通过电子邮件附近传播，它利用了人类的本性，把自己伪装成一封求爱信来欺骗收件人打开。这个病毒以其传播速度和范围让安全专家吃惊。在数小时之内，这个小小的计算机程序征服了全世界范围之内的计算机系统。

1.4.(7)“红色代码”（2001年）

被认为是史上最昂贵的计算机病毒之一，这个自我复制的恶意代码“红色代码”利用了微软 IIS 服务器中的一个漏洞。该蠕虫病毒具有一个更恶毒的版本，被称作红色代码 II 。这两个病毒都除了可以对网站进行修改外，被感染的系统性能还会严重下降。

1.4.(8)“Nimda”（2001年）

尼姆达(Nimda)是历史上传播速度最快的病毒之一，在上线之后的 22 分钟之后就成为传播最广的病毒。

1.4.(9)“冲击波”（2003年）

冲击波病毒的英文名称是 Blaster，还被叫做 Lovsan 或 Lovesan，它利用了微软软件中的一个缺陷，对系统端口进行疯狂攻击，可以导致系统崩溃。

1.4.(10)“震荡波”（2004年）

震荡波是又一个利用 Windows 缺陷的蠕虫病毒，震荡波可以导致计算机崩溃并不断重启。

1.4.(11)“熊猫烧香”（2007年）

熊猫烧香会使所有程序图标变成熊猫烧香，并使它们不能应用。

1.4.(12)“扫荡波”(2008年)

同冲击波和震荡波一样，也是个利用漏洞从网络入侵的程序。而且正好在黑屏事件，大批用户关

闭自动更新以后，这更加剧了这个病毒的蔓延。这个病毒可以导致被攻击者的机器被完全控制。

1.4.(13)“Conficker”（2008年）

Conficker.C 病毒原来要在 2009 年 3 月进行大量传播，然后在 4 月 1 日实施全球性攻击，引起全球性灾难。不过，这种病毒实际上没有造成什么破坏。

1.4.(14)“木马下载器”(2009年)

本年度的新病毒,中毒后会产生 1000~2000 不等的木马病毒,导致系统崩溃,短短 3 天变成 360 安全卫士首杀榜前 3 名(现在位居榜首)

1.4.(15)“鬼影病毒”（2010年）

该病毒成功运行后，在进程中、系统启动加载项里找不到任何异常，同时即使格式化重装系统，也无法将彻底清除该病毒。犹如“鬼影”一般“阴魂不散”，所以称为“鬼影”病毒。

1.4.(16)“极虎病毒”（2010年）

该病毒类似 qvod 播放器的图标。感染极虎之后可能会遭遇的情况：计算机进程中莫名其妙的有 ping.exe

和 rar.exe 进程，并且 cpu 占用很高，风扇转的很响很频繁（手提电脑），并且这两个进程无法结束。某些文件会出现 usp10.dll 、lpk.dll 文件，杀毒软件和安全类软件会被自动关闭，如瑞

星 、360安全卫士等如果没有及时升级到最新版本都有可能被停掉。破坏杀毒软件，系统文件，感染系统文件，让杀毒软件无从下手。极虎病毒最大的危害是造成系统文件被篡改，无法使用杀毒软件进行清理，一旦清理，系统将无法打开和正常运行，同时基于计算机和网络的帐户信息可能会被盗，如网络游戏帐户、银行帐户、支付帐户以及重要的电子邮件帐户等。

1.5 特例病毒(熊猫烧香、CIH 病毒)

1.5.1 熊猫烧香的定义特点及危害

“武汉男生”，俗称“熊猫烧香”，这是一个感染型的蠕虫病毒，它能感染系统中 exe，com，pif，src ，html ，asp 等文件，它还能中止大量的反病毒软件进程并且会删除扩展名为 gho 的文件，该文件是一系统备份工具 GHOST 的备份文件，使用户的系统备份文件丢失。被感染的用户系统中所有 .exe 可执行文件全部被改成熊猫举着三根香的模样。

熊猫烧香”其实是一种蠕虫病毒的变种，而且是经过多次变种而来的。尼姆亚变种 W(Worm.Nimaya.w)，由于中毒电脑的可执行文件会出现“熊猫烧香”图案，所以也被称为“熊猫烧香”病毒。用户电脑中毒后可能会出现蓝屏、频繁重启以及系统硬盘中数据文件被破坏等现象。同时，该病毒的某些变种可以通过局域网进行传播，进而感染局域网内所有计算机系统，最终导致企业局域网瘫痪，无法正常使用。

“熊猫烧香”（“威金”病毒变种）

病毒特征

1、这个病毒关闭众多杀毒软件和安全工具

2、循环遍历磁盘目录，感染文件，对关键系统文件跳过