网络安全 – 网络病毒防治

曹越

国家网络安全学院

武汉大学

yue.cao@whu.edu.cn

计算机病毒概述

计算机病毒的传播途径

计算机病毒对抗的基本技术

计算机病毒的清除及预防

计算机病毒概述

计算机病毒的传播途径

计算机病毒对抗的基本技术

计算机病毒的清除及预防

计算机病毒概述 – 章节分解

1. 计算机病毒介绍
2. 计算机病毒产生过程
3. 计算机病毒产生原因
4. 计算机病毒特征
5. 计算机病毒的发展简史

计算机病毒介绍 - 1

在生物学中，病毒是指侵入动植物体等有机生命体中的 具有感染性、潜伏性、破坏性的微生物，而且不同的病毒 具有不同的诱发因素。

“计算机病毒”一词是人们联系到破坏计算机系统的“病 原体”具有与生物病毒相似的特征，借用生物学病毒而使 用的计算机术语。

美国计算机安全专家Frederick Cohen博士是这样定义计 算机病毒的：”病毒程序通过修改其他程序的方法将自己 的精确拷贝或可能演化的形式放入其他程序中，从而感染它们。

计算机病毒介绍 - 2

法律依据

- **1994年2月18日，《中华人民共和国计算机信息系统安全保护条例》第二十八条**
- **计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码**

计算机病毒的判定

- **人们无法从代码上看出谁是计算机病毒，谁是正常的程序，因为计算机病毒本身就是程序。**
- **因此，计算机病毒是不可判定的，不可能用一个杀毒程序就能查出所有的病毒**

计算机病毒产生过程

程序设计

传播

潜伏

触发、运行

实施攻击

计算机病毒产生原因

一些计算机爱好者出于好奇或兴趣

产生于个别人的报复心理

来源于软件加密

产生于游戏

用于研究或实验而设计的“有用”程序，由于某种原因失去控制而扩散出来

由于政治、经济和军事等特殊目的，一些组织或个人也会编制一些程序用于进攻对方电脑

计算机病毒特征 – 感染性

- 病毒可以感染文件、磁盘、个人计算机、局部网络、互联网，病毒的感染是指从一个网络侵入另一个网络，由一个系统扩散到另一个系统，由一个系统传入到另一个磁盘，由一个磁盘进入到另一个磁盘，或者由一个文件传播到另一个文件的过程。
- 软盘、光盘、网络（主要包括电子邮件、BBS、WWW浏览、FTP文件下载等等）是计算机病毒的主要感染载体,点对点的通信系统和无线通信系统则是最新出现的病毒的感染载体。
- 感染性是病毒的再生机制，病毒通过修改磁盘扇区信息或文件内容，并与系统中的宿主程序链接在一起达到感染的目的，继而它就会在运行这一被感染的程序之后开始感染其他程序，这样一来，病毒就会很快地感染到整个系统。
- 病毒的感染性与计算机系统的兼容性有关。

计算机病毒特征 – 潜伏性

病毒的潜伏性是指其具有依附于其他媒体而寄生的能力，即通过修改其他程序而把自身的复制品嵌入到其他程序或磁盘的引导区（包括硬盘的主引导区）中寄生。

这种繁殖的能力是隐蔽的，病毒的感染过程一般都不带有外部表现，大多数病毒的感染速度极快。而且大多数病毒都采用特殊的隐藏技术，例如有些病毒感染正常程序时将程序文件压缩，留出空间嵌入病毒程序，这样使被感染病毒的程序文件的长度的变化很小，很难被发现；有些病毒修改文件的属性等；还有些病毒可以加密、变型（多态病毒）或防止反汇编、防跟踪等等都是为了不让被感染的计算机用户发现。当计算机病毒侵入系统后，一般并不立即发作，而是具有一定的潜伏期。

在潜伏期，只要条件许可，病毒就会不断地进行感染。一个编制巧妙的计算机病毒程序，可以在一段很长的时间内隐藏在合法程序中，对其他系统进行感染而不被人们发现。病毒的潜伏性与感染性相辅相成，潜伏性越好，其在系统中存在的时间就会越长，病毒的感染范围也就越大。

计算机病毒特征 – 可触发性

病毒一般都有一个触发条件：或者触发其感染，即在一定的条件下激活一个病毒的感染机制使之进行感染；或者触发其发作，即在一定条件下激活病毒的表现（破坏）部分。条件判断是病毒自身特有的功能，一种病毒一般设置一定的触发条件。

病毒程序在运行时，每次都要检测控制条件，一旦条件成熟，病毒就开始感染或发作。触发条件可能是指定的某个时间或日期、特定的用户识别符的出现、特定文件的出现或使用次数、用户的安全保密等级、某些特定的数据等等

计算机病毒特征 – 破坏性

计算机病毒的破坏性取决于病毒设计者的目的和水平

计算机病毒的危害大致有如下几个方面：

- 对计算机数据信息的直接破坏作用
- 抢占系统资源
- 影响计算机运行速度
- 病毒对计算机硬件的破坏
- 衍生性

计算机病毒特征 – 衍生性

既然计算机病毒是一段特殊的程序，了解病毒程序的人就可以根据其个人意图随意改动，从而衍生出另一种不同于原版病毒的新病毒，这种衍生出的病毒可能与原先的计算机病毒有很相似的特征，所以被称为原病毒的一个变种。

如果衍生的计算机病毒已经与以前的计算机病毒有了很大甚至是根本性的差别，则此时就会将其认为是一种新的计算机病毒。变种或新的计算机病毒可能比原计算机病毒有更大的危害性。

病毒程序与正常程序的区别

正常程序是具有应用功能的完整程序，以文件形式存在，具有合法文件名；而病毒一般不以文件的形式独立存在，一般没有文件名，它隐藏在正常程序和数据文件中，是一种非完整的程序。

正常程序依照用户的命令执行，完全在用户的意愿下完成某种操作，也不会自身复制；而病毒在用户完全不知的情况下运行，将自身复制到其他正常程序中，而且与合法程序争夺系统的控制权，甚至进行各种破坏

计算机病毒的发展简史 - 1

1949年，计算机之父冯•诺依曼在《复杂自动机组织论》中提出“一部事实上足够复杂的机器能够复制自身”。

20世纪60年代初，美国贝尔实验室里“磁芯大战”的游戏。1975年，《Shock Wave Rider》(John Bruner)出现了“Virus”一词。

1981年，世界上诞生了真正意义上的计算机病毒—Elk Cloner，这个病毒将自己附着在磁盘的引导扇区上，通过磁盘进行感染。

1983年11月3日，美国计算机安全学术讨论会上，Frederick Cohen博士首次提出计算机病毒的概念。同一天，专家们在VAX11/750计算机系统上验证了计算机病毒的存在。在其后的一周内，在5次病毒试验中，平均30分钟病毒就可使计算机系统瘫痪。

计算机病毒的发展简史 - 2

1986年底，病毒Brain开始流行。Brain病毒首次使用了伪装的手段来迷惑计算机用户。1987年10月，美国新闻机构报道了这一事件。

在这一年，中国的公安部成立了计算机病毒研究小组，并派出专业技术人员到中科院计算所和美国、欧洲进修、学习计算机安全技术，标志着计算机病毒引起了中国政府的警惕。

1987年，DOS环境下的文件型病毒得到了很大的发展。出现了能自我加解密的病毒—Cascade，Stoned病毒和PingPong病毒等等。同年12月份，第一个网络病毒—Christmas Tree开始流行。

计算机病毒的发展简史 - 3

1988年11月2日，美国康奈尔大学的学生Morris将自己编制的蠕虫程序在几小时内造成Internet网络的堵塞，6000多台计算机被感染，造成巨大的损失。在美国，仅1988年中，就约有9万台计算机遭计算机病毒入侵。《人民日报》就Morris 事件报道了关于病毒的事件。

同时，反病毒技术也已经开始成熟了，所罗门公司的反病毒工具——Doctors Solomon‘s Anti-Virus Toolkit—成为当时最强大的反病毒软件。

1989年，病毒家族开始出现了，比如Yankee病毒，Eddie病毒，Frodo病毒（第一个全秘密寄生的文件病毒）。同年出现了名为AIDS的特洛伊木马型病毒。

计算机病毒的发展简史 - 3

1989年4月西南铝厂首先发现小球病毒，计算机病毒开始侵入我国。

1989年7月，中国公安部推出了中国最早的杀毒软件Kill6.0。

1990年，出现了第一个多态病毒Chameleon、使用多级加密解密和反跟踪技术的病毒Whale等，可以用于开发病毒的工具软件——VirusProductionFactory，专门为病毒制造者开设的进行病毒信息交流和病毒交换的BBS。

介入杀毒市场。中国的瑞星公司成立，推出了瑞星防病毒卡。

1992年，多态病毒生成器“MtE”开发出来，病毒构造工具集VirusCreateLibrary开发成功。在芬兰发现了首例Windows病毒。

计算机病毒的发展简史 - 4

1995年8月9日，在美国首次发现专门攻击Word文件的宏病毒——Concept。

1997年2月，第一个Linux环境下的病毒Bliss出现。1997年4月，第一个使用FTP进行传播的Homer病毒出现。

1998年6月，CIH病毒被发现。这一年也出现了远程控制工具“BackOrifice”、“Netbus”等，第一个感染Java可执行文件的StrangeBrew病毒，用实用VB脚本语言编写的Robbit病毒。

1999年，通过邮件进行病毒传播开始成为病毒传播的主要途径，而宏病毒仍然是最流行的病毒。这一年，比较有名的病毒有：Melissa，Happy99；FunLove等等。

1993年、1994年，采用密码技术、编写技巧高超的隐蔽型病毒和多态性病毒相继出现，也出现了感染源代码文件的SrcVir病毒和感染OBJ文件的Shifter病毒。

计算机病毒的发展简史 - 5

2000年被称作VBScript病毒/蠕虫之年。大量使用脚本技术的病毒出现，脚本技术和蠕虫、传统的病毒、木马程序以及操作系统的安全漏洞相结合，给病毒技术带来了一个新的发展高峰。最著名的如VBS/KAK蠕虫，Loveletter病毒。2000年，中国的金山公司发布金山毒霸，金山公司开始进入杀毒软件市场。

2001年7月出现了Code Red和Code Red II，9月出现的Nimda病毒突破了以往病毒的各种传播途径，它们会利用微软服务器漏洞植入后门程序的特洛伊木马，或是通E-mail大肆传播、衍生无数变种的计算机蠕虫，也有可能是通过浏览网页下载病毒，甚至三者兼具，造成了大范围的因特网上的服务器被阻断或访问速度下降，在世界范围内造成了巨大的损失。仅Code Red病毒所造成的经济损失，就远远超过过去6年来任何一年的年度损失。

计算机病毒的发展简史 - 6

开始时传播速度和范围没达到西方的规模，时间上滞后。

随着计算机网络在中国的普及，计算机病毒在中国的出现逐步与世界“接轨”。

中国越来越多地出现了“国产病毒”（“新世纪”、“中国炸弹”、“冰河”等)

防病毒的水平相对较差。

计算机病毒概述

计算机病毒的传播途径

计算机病毒对抗的基本技术

计算机病毒的清除及预防

计算机病毒感染的途径 – 章节分解

1. 计算机病毒感染的途径
2. 计算机病毒划分
3. 引导型病毒特点
4. 文件型病毒特点
5. 计算机病毒存在方式
6. 病毒程序的组成
7. 计算机病毒基本原理
8. 病毒的隐藏（欺骗）技术

计算机病毒感染的途径

- 引进的计算机系统和软件中带有病毒
- 各类出国人员带回的机器和软件染有病毒
- 染有病毒的游戏软件
- 非法拷贝中毒
- 计算机生产、经营单位销售的机器和软件染有病毒
- 维修部门交叉感染
- 有人研制、改造病毒
- 敌对分子以病毒为媒体或武器进行宣传和破坏
- 通过互联网（访问Web、下载Email和文件等）传入的

计算机病毒划分 - 1

按攻击平台划分

- **攻击DOS系统的病毒**
- **攻击WINDOWS系统的病毒**
- **攻击UNIX/Linux系统的病毒**
- **攻击IBM OS/2系统的病毒**
- **攻击Mac系统的病毒**
- **其它操作系统上的病毒（如手机病毒）**

计算机病毒划分 - 2

按链接方式划分

- **源码型病毒**
- **嵌入型病毒**
- **Shell病毒**
- **译码型病毒（如宏病毒，脚本病毒）**
- **操作系统型病毒**

计算机病毒划分 - 3

按破坏情况划分

- 良性病毒
- 恶性病毒

按传播媒介划分

- 单机病毒
- 网络病毒

按寄生方式和传染途径划分

- 引导型病毒
- 文件型病毒
- 引导型兼文件型病毒

引导型病毒特点

引导型病毒特点

- 引导部分占据磁盘引导区
- 只有在计算机启动过程中，磁盘被引导时，“引导型”病毒才被激活
- 具有磁盘引导扇区内容“复原”功能
- 修改内存容量，病毒驻留内存
- 修改磁盘访问中断，在进行磁盘写操作的时候进行传播

引导型病毒传播方式

- 正常的操作系统启动过程
- 感染引导型病毒的操作系统启动

文件型病毒特点

文件型病毒的主要特点是：

- 系统执行病毒所寄生的文件时，其病毒才被激活
- 有可能直接攻击目标对象，主要是EXE、COM等可执行文件，如果是混合型病毒，则还要攻击硬盘的主引导扇区或操作系统引导扇区
- 修改系统内存分配，病毒驻留内存
- 修改系统中断，等待时机进行病毒的发作或再次传播

计算机病毒存在方式

静态

- 存在于辅助存储介质上的计算机病毒
- 静态病毒不能产生传染和破坏作用

动态

- 进入了计算机内存的计算机病毒
- 内存中的动态病毒又有两种状态：能激活态和激活态

失活态

- 用户的干预下，内存中的病毒代码不能被系统的正常运行机制执行

病毒程序的组成

感染模块

触发模块

破坏模块

主控模块

病毒程序的组成 – 感染模块

感染模块

- 寻找可执行文件
- 检查文件是否有感染标记
- 将病毒代码放入宿主程序

感染机制有寄生感染，插入感染和逆插入感染，链式感染，破坏性感染，滋生感染，没有入口点的感染，OBJ、LIB和源码的感染，混合感染和交叉感染，零长度感染等

病毒程序的组成 – 触发模块

触发模块

- **触发模块根据预定条件满足与否，控制病毒的感染或破坏动作**
- **病毒的触发条件有多种形式，例如：日期、时间、键盘、发现特定程序、感染的次数、特定中断调用的次数等**

病毒程序的组成 – 破坏模块

破坏模块

- **破坏模块负责实施病毒的破坏动作，其内部是实现病毒编写者预定破坏动作的代码**
- **表现模块：有些病毒的该模块并没有明显的恶意破坏行为，仅在被传染的系统设备上表现出特定的现象，该模块有时又被称为表现模块**

常见的破坏有

- **攻击系统数据区，攻击文件和硬盘， 攻击内存，干扰系统的运行，扰乱输出设备，扰乱键盘，修改注册表，干扰上网，以及降低系统性能**

病毒程序的组成 – 主控模块 1

主控模块

- **流程**

1. **调用感染模块，进行感染**
2. **调用触发模块，接受其返回值**
3. **如果返回真值，执行破坏模块**
4. **如果返回假值，执行后续程序**

病毒程序的组成 – 主控模块 2

主控模块

- **调查运行的环境: 以IBM PC机病毒为例，病毒主控模块要确定内存容量、现行区段、磁盘设置、显示器类型等参数**
- **常驻内存的病毒要做包括请求内存区、传送病毒代码、修改中断向量表等动作**
- **病毒在遇到意外情况时，必须能流畅运行，确保不出现死锁。**
  - **例如病毒程序欲感染宿主程序，但磁盘已经写不下或者磁盘处于写保护状态。**
  - **如果不做妥善处理，病毒不能运行，而且操作系统的报警信息也可能使病毒暴露**

计算机病毒基本原理

- DOS病毒
- 宏病毒
- 脚本病毒
- PE病毒

计算机病毒基本原理 – DOS病毒 1

引导区病毒

文件型病毒

混合型病毒

计算机病毒基本原理 – DOS病毒 2

引导区病毒

- **主引导记录是用来装载硬盘活动分区的BOOT扇区的程序**
- **主引导记录存放于硬盘0面0道1扇区，长度一般为一个扇区**
- **按寄生对象：主引导区病毒、引导区病毒**

计算机病毒基本原理 – DOS病毒 3

引导型病毒的主要特点1

- **引导型病毒是在安装操作系统之前进入内存，因此不得不采用减少操作系统所掌管的内存容量方法来驻留内存高端**

计算机病毒基本原理 – DOS病毒 4

引导型病毒的主要特点2

- **引导型病毒感染硬盘时，必定驻留硬盘的主引导扇区或引导扇区，并且只驻留一次，因此引导型病毒一般都是在软盘启动过程中把病毒传染给硬盘的**
- **引导型病毒的寄生对象相对固定，把当前的系统主引导扇区和引导扇区与干净的主引导扇区和引导扇区进行比较，如果内容不一致，可认定系统引导区异常**

计算机病毒基本原理 – DOS病毒 5

文件型病毒

- **通过操作系统的文件系统进行感染的病毒都称作文件病毒**
- **批处理文件、DOS下的可加载驱动程序（.SYS）文件以及普通的COM / EXE可执行文件、带毒源程序**

计算机病毒基本原理 – 宏病毒 1

宏病毒是使用宏语言编写的程序，可以在一些数据处理系统中运行（主要是微软的办公软件系统，字处理、电子数据表和其他Office程序中）

存在于字处理文档、数据表格、数据库、演示文档等数据文件中，利用宏语言的功能将自己复制，并且繁殖到其他数据文档里

计算机病毒基本原理 – 宏病毒 2

原理

- 使用微软的字处理软件Word，用户可以进行打开文件、保存文件、打印文件和关闭文件等操作。在进行这些操作的时候，Word软件会查找指定的“内建宏”，不过这些宏只对当前文档有效
- 另外还有一些以“自动”开始的宏，比如说“AutoOpen”、“AutoClose”等，如果这些宏定义存在的话，打开/关闭文件的时候会自动执行这些宏，这些宏一般是全局宏。
- 在Excel环境下同样存在类似的自动执行的宏

计算机病毒基本原理 – 脚本病毒 1

脚本病毒种类比较多，比较常见的就是VBS病毒

VBS病毒是用VBScript编写而成，该脚本语言功能非常强大

它们利用Windows系统的开放性特点，通过调用一些现成的Windows对象、组件，可以直接对文件系统、注册表等进行控制

计算机病毒基本原理 – 脚本病毒 2

原理

- **VBS脚本病毒是直接通过自我复制来感染文件的，病毒中的绝大部分代码都可以直接附加在其他同类程序的中间**

VBS病毒特点

- **编写简单，破坏力大，感染力强，传播范围大，病毒源码容易被获取，变种多，欺骗性强，实现病毒生产机非常容易**

计算机病毒基本原理 – 脚本病毒 3

传播方式

- **Email, 局域网共享, 感染html等网页文件, 聊天通道**

如何获得控制权

- **修改注册表项，映射文件执行方式，欺骗用户让用户执行，desktop.ini和folder.htt**

对抗技巧

- **自加密，Execute，改变声明，关闭反病毒软件**

计算机病毒基本原理 – 脚本病毒 4

VBS脚本病毒的弱点

- **绝大部分VBS脚本病毒运行的时候需要用到一个对象：FileSystemObject**
- **VBScript代码是通过Windows Script Host来解释执行的**
- **VBS脚本病毒的运行需要其关联程序Wscript.exe的支持**
- **通过网页传播的病毒需要ActiveX的支持**
- **通过Email传播的病毒需要OutlookExpress的自动发送邮件功能支持，但是绝大部分病毒都是以Email为主要传播方式的**

计算机病毒基本原理 – 脚本病毒 5

VBS脚本病毒的防范

- **禁用文件系统对象FileSystemObject**
- **卸载Windows Scripting Host**
- **Wscript.exe改名**
- **自定义安全级别、禁止OutlookExpress等**
- **不关联VBS，JSE等文件后缀名与应用程序映射**
- **杀毒软件**

计算机病毒基本原理 – PE病毒

Win PE格式病毒

关键技术

1. **病毒的重定位**
2. **获取API函数地址**
3. **文件搜索**
4. **感染其他文件**
5. **返回到Host程序**

计算机病毒传播途径

流行传播途径

- **网页**
- **Email**
- **局域网共享、共享的个人计算机**
- **漏洞**
- **对等网络应用软件**
- **盗版软件等**

新一代计算机病毒的特点及发展趋势

- 多种方式传播，传播速度极快
- 利用微软漏洞主动传播
- 更广泛的混合性特征
- 病毒与黑客技术的融合
- 欺骗性增强
- 病毒出现频度高，生成工具多，变种多
- 危害性极大，大量消耗系统与网络资源
- 难于控制和彻底根治，容易引起多次疫情

病毒的隐藏（欺骗）技术 - 1

病毒的反跟踪技术

病毒的加密及多态

宏病毒、脚本病毒和邮件病毒的隐藏（欺骗）技术

病毒的隐藏（欺骗）技术 - 2

病毒的隐藏技巧，贯穿于3个模块（引导、感染、表现）之中，使病毒在运行过程中直到其表现（破坏）发作以前都尽可能地不被人发觉。引导型病毒、文件型病毒采用了不同的技术达到这个目的。

病毒的隐藏（欺骗）技术 - 3

- 一是改变BIOS中断INT13H的入口地址，使其指向病毒代码之后，发现调用INT13H读取被感染扇区的时候，将原来的没有被感染的内容返回给调用的程序，这样，任何DOS程序都无法觉察到病毒的存在；
- 另一方法是针对杀毒软件的，病毒在加载程序的时候制造假相，当系统启动任何程序的时候，病毒修改DOS执行程序的中断，先把被病毒感染的扇区恢复原样，这样，即使反病毒软件采用直接访问磁盘的方法也觉察不到病毒的存在，当程序执行完成后再重新感染。
- 引导型病毒还经常采用更改活动记录、使病毒代码看起来非常类似正常启动代码等方法隐藏自身。

病毒的隐藏（欺骗）技术 - 4

文件型病毒除了与引导型病毒相类似的方法之外，还要考虑到其他方面，因为操作系统访问文件的方法非常多。

所以一个完整的隐藏技术，应该包括下面几个方面的处理：

- 系统列目录时显示感染前的文件大小
- 读写文件看到正常的文件内容
- 执行或搜索时隐藏病毒
- 在支持长文件名的系统中隐藏自身、隐藏病毒扇区等

病毒的反跟踪技术

- 抑制跟踪命令
- 定时技术
- 封锁键盘输入

病毒的加密及多态

病毒加密的目的主要是防止跟踪或掩盖有关特征等，这就给病毒的检测和杀除带来了难度，也能使病毒更好地隐藏。对付这种病毒的一个有效方法是采取虚拟执行技术。

加密的方法很多，很多方法既简单易行，又难于破解，这些方法被病毒制造者们充分地利用起来。

计算机病毒概述

计算机病毒的传播途径

计算机病毒对抗的基本技术

计算机病毒的清除及预防

计算机病毒对抗的基本技术 – 章节分解

- 计算机病毒对抗的基本技术概述
- 常规计算机病毒的检测内容
- 特征值检测技术
- 校验和检测技术
- 启发式扫描技术
- 虚拟机技术

计算机病毒对抗的基本技术概述

计算机病毒危害计算机本身的安全和信息安全

病毒对抗主要研究病毒的检测、病毒的清除和病毒的预防

病毒的检测技术主要有特征值检测技术、校验和检测技术、行为监测技术、启发式扫描技术、虚拟机技术

常规计算机病毒的检测内容

常规计算机病毒的检测内容

- **主引导区（坏区，中断向量）**
- **可执行文件（程序头部）**
- **内存空间（内存空间是否被覆盖）**
- **根据特征值查找（特殊字符串）**

特征值检测技术 - 1

特征值检测技术

- **病毒标识**
- **从而对宿主仅感染一次**
- **计算机病毒的特征值可能有别于病毒标识，特征值是指一种病毒有别于另一种病毒的字符串**

优缺点

- **误报率低**
- **不能检测未知病毒**

校验和检测技术 - 1

校验和检测技术

- **计算正常文件的内容和正常的系统扇区的校验和，将该校验和写入数据库中保存。**
- **在文件使用/系统启动过程中，检查文件现在内容的校验和与原来保存的校验和是否一致，因而可以发现文件/引导区是否感染**

校验和检测技术 - 2

校验和检测技术特点

- **这种方法既能发现已知病毒，也能发现未知病毒，但不能识别病毒种类**
- **由于病毒感染并非是文件内容改变的唯一原因，文件内容的改变有可能是正常程序引起的，所以校验和检测技术常常误报警**
- **而且此种方法也会影响文件的运行速度**

校验和检测技术 - 3

校验和检测技术实现方式

1. **在检测病毒工具中纳入校验和检测技术，对被查对象文件计算其正常状态的校验和，将校验和值写入被查文件中或检测工具中，而后进行比较**
2. **在应用程序中，放入校验和检测技术自我检查功能，将文件正常状态的校验和写入文件本身中，每当应用程序启动时，比较现行校验和与原校验和值，从而实现应用程序的自检测**
3. **将校验和检查程序常驻内存，每当应用程序开始运行时，自动比较检查应用程序内部或别的文件中预先保存的校验和**

校验和检测技术 - 4

校验和检测技术实现方式

- **优点：简单，能发现未知病毒**
- **缺点：需要预先记录正常文件校验和，不能识别病毒名称，抗隐蔽性差**

病毒行为监测技术

病毒行为监测技术

- **不论如何伪装，总会引起与正常程序不同行为（如不断复制达到传播目的）**
- **尽管正常程序有此行为，只有病毒才会同时具有多种病毒性为利用此特点，利用此特点，可对病毒实施监视，预警**

优缺点

- **可发现未知病毒，可相当准确预测未知病毒**
- **误警率高，不能识别病毒名字。**

启发式扫描技术 - 1

介绍

- 是一种概率方法
- 按照安全、可疑等级对操作进行排序（比如病毒格式化磁盘的操作可疑度等级高）
- 如果一个程序的加权值超过阈值，判定为病毒

优缺点

- 可发现未知病毒，可相当准确预测未知病毒
- 误警率高，不能识别病毒名字

启发式扫描技术 - 2

在具体实现上，启发式代码扫描技术是相当复杂的。

通常这类病毒检测软件要能够识别并探测许多可疑的程序代码指令序列，如格式化磁盘类操作，搜索和定位各种可执行程序的操作，实现驻留内存的操作，发现非常的或未公开的系统功能调用的操作，等等，所有上述功能操作将被按照安全和可疑的等级排序，根据病毒可能使用和具备的特点而授以不同的加权值。

启发式扫描技术 - 3

为了方便用户或研究人员直观地检测被测试程序中可疑功能调用的存在情况，病毒检测程序可以显示不同的可疑功能调用设置标志。

对于某个文件来说，被点亮的标志愈多，染毒的可能性就愈大。常规干净程序甚至很少会点亮一个标志旗，但如果要作为可疑病毒报警的话，则至少要点亮两个以上标志旗。如果再给不同的标志旗赋予不同的加权值，情况还要复杂得多。

启发式扫描技术 - 4

传统扫描技术由于基于对已知病毒的分析和研究，在检测时能够更准确，减少误报，但如果是对待此前根本没有见过的新病毒，由于传统手段的知识库并不存在该类（种）病毒的特征数据，则有可能造成漏报。

而这时基于规则和定义的启发式代码分析技术，则正好可以大显身手，使这类新病毒不至于成为漏网之鱼。传统与启发式技术的结合使用，可以使病毒检测软件的检出率达到很高的水平，而另一方面，又大大降低了总的误报率。

某种病毒能够同时逃脱传统和启发式扫描分析的可能性是小的，如果两种分析的结论相一致，那么真实的结果往往就如同其判断结论一样确定无疑。

虚拟机技术

虚拟机技术

- 多态性病毒每次感染都改变其病毒密钥，普通特征值检测方法失效
- 对其代码实施加密变换，每次不同密钥，不容易找出相同的特征值
- 病毒执行时候，需要对自身进行还原，为此让病毒程序在虚拟机上运行，原形毕露

优缺点

- 单纯的静态分析进入了动态+静态集合的竞价，提高了检测水平

计算机病毒概述

计算机病毒的传播途径

计算机病毒对抗的基本技术

计算机病毒的清除及预防

计算机病毒的清除及预防 – 章节分解

1. 病毒的清除概述
2. 引导型病毒的清除
3. 文件型病毒的清除
4. 宏病毒的清除
5. 病毒的去激活
6. 计算机病毒的常规预防
7. 计算机系统修复应急计划

病毒的清除概述 - 1

将染毒文件的病毒代码摘除，使之恢复为可正常运行的健康文件，称为病毒的清除

不是所有染毒文件都可以消毒，也不是所有染毒系统都能够驱除病毒使之康复

不论手工消毒还是用抗病毒软件进行消毒，都是危险操作，可能出现不可预料的结果，将染毒文件彻底破坏

病毒的清除概述 - 2

- 无毒环境
- 杀毒盘写保护
- 准确判断病毒的种类
- 尽量不用激活病毒的方法检测病毒和病毒标识免疫方法清除病毒
- 杀毒工作要深入而全面
- 交叉感染或重复感染的，要按感染的逆顺序从后向前依次清除

引导型病毒的清除

引导型计算机病毒主要是感染磁盘的引导扇区。

我们在使用被感染的磁盘（无论是软盘还是硬盘）启动计算机时它们就会首先取得系统控制权，驻留内存之后再引导系统，并伺机传染其他软盘或硬盘的引导区。纯粹的引导型计算机病毒一般不对磁盘文件进行感染。

引导型病毒的清除（病毒不在RAM）

文件型病毒的清除

文件型计算机病毒通过修改.COM、.EXE等文件的结构，将计算机病毒代码插入到宿主程序，文件被感染后，长度、日期和时间等大多发生变化，也有些文件型计算机病毒传染前后文件长度、日期、时间不会发生任何变化，称之为隐型计算机病毒。隐型计算机病毒是在传染后对感染文件进行数据压缩，或利用可执行文件中有一些空的数据区，将自身分解在这些空区中，从而达到不被发现的目的。

文件型病毒的清除

- 不区分文件的属性（只读/系统/隐藏），测试和恢复所有的目录下的可执行文件
- 确保文件的属性和最近修改时间不改变
- 一定考虑一个文件多重感染情况

宏病毒的清除

- 在没打开任何文件（文档文件或模板文件）的情况下，启动Word；
- 选择菜单“工具 / 模板和加载”项中的“管理器 / 宏方案”项；
- 删除左右两个列表框中除了自己定义的之外的所有宏；
- 关闭对话框；
- 选择菜单“工具 / 宏”，若有AutoOpen，AutoNew，AutoClose等宏，则加以删除；

病毒的去激活

病毒的去激活

1. **检测病毒执行过程**
2. **改变执行方式**
3. **使病毒失去传染力**
4. **消除病毒的恢复机制**

计算机病毒的常规预防

- 检查外来文件，小心运行可执行文件
- 局域网预防（断网检查）
- 使用确认和数据完整性工具（大小，时间，属性）
- 留心计算机出现的异常
- 及时升级抗病毒工具的病毒特征库和杀毒引擎
- 购买正版软件
- 周期性备份工作文件
- 建立健全安全管理制度

引导型病毒的预防

引导型病毒的特征

- **引导型病毒一般在启动计算机时，优先取得控制权，强占内存。**

预防引导型病毒的方法：

- **尽量不用软盘或用干净的软盘启动系统。**
- **对软盘进行写保护。**
- **用软件来保护硬盘。**

文件型病毒的预防

文件型病毒的特征：

- **凡是文件型病毒，都要寻找一个宿主，寄生在宿主“体内”，然后随着宿主的活动到处传播。这些宿主基本都是可执行文件。**

预防文件型病毒的方法：

- **常驻内存监视INT 21H中断，给可执行文件加上“自检外壳”等。**
- **还可以使用专用程序给可执行文件加上“自检外壳”的方法。**
- **在源程序中增加自检及清除病毒的功能。**

宏病毒的预防

宏病毒的特征：

- **主要针对微软的Office软件进行侵袭。**

预防宏病毒的方法：

- **根据AUTO宏的自动执行的特点，在打开Word文档时，可通过禁止所以自动宏的执行办法来达到防治宏病毒的目的**
- **当怀疑系统带有宏病毒时，首先应检查是否存在可疑的宏，也就是一些用户没有编制过、也不是Word默认提供而出现的的宏，特别是出现一些奇怪名字的宏，如AAAZA0等，肯定是病毒无疑，删除即可**
- **当使用外来可能有宏病毒的Word文档时，如果没有保留原来文档排版格式的必要，可先使用Windows自带的写字板来打开，将其转换为写字板格式的文件保存后，再用Word调用**

个性化的预防措施

病毒的感染总是带有普遍性的或大众化的，以使传染的范围尽可能的广，所以有时一些个性化的处理可能对病毒的预防或免疫具有非常好的效果。

例如给一些系统文件改名（或扩展名）；对一些文件（甚至子目录）加密，使得病毒搜索不到这些系统文件。

计算机系统修复应急计划 - 1

1-人员准备

- 首先需要指定一个全局的负责人，一般由领导担当，负责各项工作的分配和协调。参加应急工作的人员一般应包括：网络管理员、技术负责人员、设备维护管理人员和使用者（用户）或值班用户
- 在发现新的计算机病毒疫情后，可以通过防杀计算机病毒厂商及寻求计算机病毒防范专家的支持

计算机系统修复应急计划 - 2

2-应急计划的实施步骤

- 对染毒的计算机和网络进行隔离
- 向主管部门汇报计算机病毒疫情
- 确定计算机病毒疫情规模
- 破坏情况估计及制定抢救策略
- 实施计算机网络系统恢复计划和数据抢救恢复计划

3-善后工作

- 将网络恢复正常运作，并总结发生计算机病毒疫情后的应急计划实施情况和效果，不断修改应急计划，使得它能够根好地解决问题，降低损失。

4-其他

- 在应急计划中还必需包括救援物质、计算机软硬件备件的准备，以及参加人员的联络表等，以便使得发生计算机病毒疫情后能够迅速地召集人手，备件到位，快速进入应急状态。

课后问题

1. 计算机病毒的定义和特征

2. 宏病毒采用哪些传播方式?

3. 阐述病毒检测的主要技术

4. 根据自己的感受，给出病毒预防的基本策略

谢谢!