网络安全 – 计算机病毒

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 - 1

生物病毒

- **一种微小的基因代码段—DNA或RNA，它能掌管活细胞机构，并采用欺骗性手段生成成千上万的原病毒的复制品**

计算机病毒

- **一段附着在其它程序上的、可以自我繁殖的程序代码**

计算机病毒概述 - 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 - 1

传染性

- 病毒具有把自身复制到其它程序的能力

非授权性

- 病毒程序的执行对用户是未知的，即病毒的执行具有某种主动性

隐蔽性

- 用户不容易察觉病毒程序的存在与执行

计算机病毒特征 - 2

潜伏性

- **病毒存在于系统中，并等待时机发作**

破坏性

- **干扰系统的执行、管理、数据**

不可预见性

可触发性

- **根据条件触发破坏行动**

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

- 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
- 检查文件是否又感染标记
- 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htm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**

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 - 1

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

计算机病毒对抗的基本技术 - 2

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）**

计算机病毒对抗的基本技术 - 3

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**

计算机病毒对抗的基本技术 - 4

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**

计算机病毒对抗的基本技术 - 5

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，但是，它不能识别病毒种类**
- **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**

计算机病毒对抗的基本技术 - 6

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**

计算机病毒对抗的基本技术 - 7

新技术

- 病毒行为监测技术
  - 可能误报，不实时
- 启发式扫描技术
  - 分析文件中的指令序列，根据统计知识，判断被感染概率
- 虚拟机技术
  - 让病毒程序在虚拟机上运行，原形毕露

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

病毒的清除 - 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 - 2

引导型病毒的清除（病毒不在RAM）

- **SYS**
- **fdisk /mbr /pri:x x**

宏病毒的清除

- **RTF(Rich Text Format)**

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**

病毒的清除 - 3

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

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!