大学生计算与信息化素养

恶意代码及网络防病毒技术

本次课程所讲内容

- 恶意代码
- 网络防病毒技术
- 养成良好的信息安全意识

恶意代码

恶意代码又称恶意软件，是指故意编制或设置的、对网络或系统会产生威胁或潜在威胁的计算机代码。

恶意代码能够从一台计算机传播到另一台计算机，从一个网络传播到另一个网络，目的是在用户和网络管理员不知情的情况下对系统进行故意地修改。

最常见的恶意代码有计算机病毒（简称病毒）、特洛伊木马（简称木马）、计算机蠕虫（简称蠕虫）、后门、逻辑炸弹等。

恶意代码发展阶段

- 第一代
  - DOS病毒（1986年～1995年）
- 第二代
  - 宏病毒（1995年～2000年）
- 第三代
  - 网络蠕虫病毒（1999年～2004年）
- 第四代
  - 趋利性恶意代码（2005年～至今）

恶意代码

恶意代码具有如下三个共同的特征：恶意的目的、本身是程序、通过执行发生作用。

恶意代码的传播手段：编写者一般利用三类手段来传播恶意代码：软件漏洞、用户本身或者两者的混合。

恶意代码的传播趋势：Windows操作系统、多平台、种类模糊、混合传播模式和恶意代码类型变化、使用销售技术。

网络安全技术

网络安全技术研究的基本问题包括：网络防攻击、网络安全漏洞与对策、网络中的信息安全保密、网络内部安全防范、网络防病毒、网络数据备份与灾难恢复。

网络防病毒系统的基本结构

网络防病毒系统通常是由系统中心、服务器端、工作站、管理控制台等子系统组成。

网络防病毒技术

1. **病毒预防技术**，就是通过一定的技术手段对病毒的规则进行分类处理，而后在程序运作中凡有类似的规则出现，则认定是计算机病毒。通过阻止计算机病毒进入系统内存或阻止计算机病毒对磁盘的操作，尤其是写操作。

2. **病毒检测技术**，是指通过技术手段判定出特定的计算机病毒。它包括两类：一种是根据病毒的特征及传染方式等，在特征分类的基础上建立的病毒检测技术。另一种是不针对具体病毒程序的自身校验技术。

网络防病毒技术

3. **病毒清除技术**，计算机病毒的清除技术是计算机病毒传染程序的一种逆过程。目前，清除病毒大都是在某种病毒出现后，通过对其进行分析研究而研制出来的具有相应解毒功能的软件。

要使网络有序、安全的运行，必须加强网络使用方法、网络安全技术与道德教育，完善网络管理，研究与开发新的网络安全技术与产品。

防病毒软件

病毒查杀能力是衡量网络版杀毒软件性能的重要因素。用户在选择软件的时候不仅要考虑可查杀病毒的种类数量，更应该注重其对流行病毒的查杀能力及对新病毒的反应能力。

产品：瑞星、金山毒霸、江民、卡巴斯基、诺顿、安全卫士360、、微点、McAfee等。

养成良好的信息安全意识

1.在使用移动介质（如：U盘、移动硬盘等）之前，建议先进行病毒查杀；

2.禁用系统的自动播放功能，防止病毒从U盘、移动硬盘等移动存储设备进入到计算机；

3.不要关闭防病毒等终端防护系统；

4.及时给计算机的防病毒及终端安全防护软件升级；

5.邮件带有附件的应另存后再打开，不要直接打开；

6.使用安全密码策略，建议至少使用4个字母（包括大小写）和4个数字的组合密码

养成良好的信息安全意识

7.不要轻易打开及时通信工具上发送的链接；

8.不要下载和安装来历不明的软件；

9.不要浏览不明网页；

10.不要使用桌面和系统默认的目录存放重要文件，对重要数据经常备份；

11. 在登录电子银行实施网上查询交易时，尽量选择安全性较高的USB证书认证方式。不要在公共场所(如网吧)登录网上银行等一些金融机构的网站，防止重要信息被盗。