软件安全—恶意代码机理与防护

C3 PE文件格式

武汉大学计算机学院 彭国军

guojpeng@whu.edu.cn

本讲的内容提纲

3.1 PE文件及其表现形式
3.2 PE文件格式与恶意软件的关系
3.3 PE文件格式总体结构
3.4 代码节与数据节
3.5 引入函数节：PE文件的引入函数机制
3.6 引出函数节：DLL文件的函数引出机制
3.7 资源节：文件资源索引、定位与修改
3.8 重定位节：镜像地址改变后的地址自动修正

3.2 PE文件格式与恶意软件的关系

- 何为文件感染？［或控制权获取］
  - 使目标PE文件具备［或启动］病毒功能［或目标程序］
  - 但不破坏目标PE文件原有功能和外在形态（如图标）等
- 病毒代码如何与目标PE文件融为一体？
  - 代码植入、
  - 控制权获取、
  - 及图标更改等。