软件安全—恶意代码机理与防护

C3 PE文件格式

彭国军 教授

武汉大学国家网络安全学院

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
3.9 PE文件数字签名与验证机制
3.10 ELF文件格式

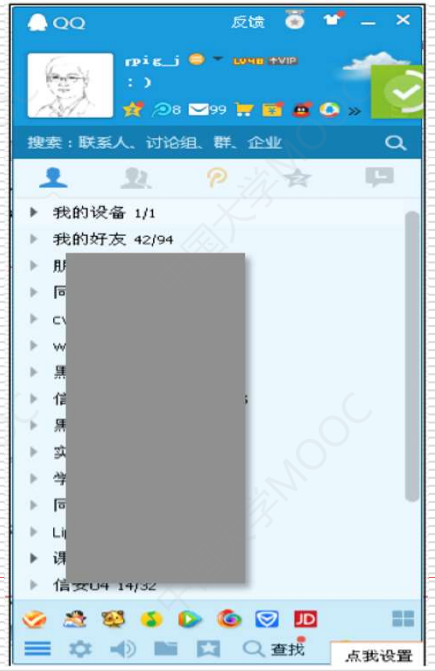
3.1 PE文件及其表现形式

- 可移植的可执行文件（PE，Portable Executable File），Win32平台可执行文件使用的一种格式。

- 其他EXE文件格式：
  - DOS：MZ格式
  - Windows 3.0/3.1：
    - NE，New Executable
    - 16位Windows可执行文件格式

可执行程序的不同形态（以QQ为例）

- 用户眼中的QQ.



可执行程序的不同形态（以QQ为例）

- 本质上