Chapter 7 Malicious Code 恶意代码

2017年4月10日 10:46

BY LSY

Overview:

- type——Trojans, viruses, worms, others
- defenses of malicious code
- botnets, spam and DDoS

1. Trojans 木马
   - Trojan Horse 特洛伊木马
     - program with an overt purpose(known to user) and a covert purpose(隐通道) (unknown to user)
     - 可以自我繁殖
     - hard to detecta
   - Trojan Compiler
   - Trojan concealing ——Roootkit 如何隐藏自己
     - 把可以查到的e. g. 进程管理器都隐藏掉，将黑客信息与用户屏蔽开

2. Computer Virus 病毒
   - 病毒依附于可执行程序exe（如果被插入的程序不执行病毒就不会执行），木马是独立的可执行程序
   - 满足传播条件
     - 传遍目标
       - 如果传播目标没有被影响
         - 确定哪里插入病毒
         - 插入
         - 执行
   - Boot Sector Infectors 启动引导分区病毒，即在电脑启动程序中插入
   - Executable Infectors 执行程序.exe中将病毒插入到头之后，真正的程序往后移，源程序不会崩溃
     - 插入方式不做要求！！！
     - Means of attaching 执行程序.exe中将病毒插入到头之后,将被覆盖的源代码删除掉，后面的程序damage直接崩溃
     - 插到末尾，先跳过去再跳回原来的程序
   - 加密病毒密码，很难被找到——看deciphering key来找
   - Anti-virus tool不仅需要找到病毒，还需要知道是哪一种病毒

3. Worm 蠕虫
   - 不断随机扫描IP看是不是活着
   - 爆发性增长
     - slammer's influence
     - blaster worm
     -
     - welchia/nachia

4. Defence
   - clear distinction between data and executable
     - virus必须需要改变执行代码, write to program, 可执行端和数据端分开
       - write only allowed to data
     - limiting accessiblity
     - application of principle of least priviledge

    - guardians, watchdogs 监测和介入文件的修改
    - sandbox/virtual machine
        - 防止恶性网站修改/破坏本地
- defence means
    - detect alteration of files， 检测对文件的修改
    - defenses means
        - detect actions beyond specifications, 根据行为来进行检测
        - 在库里进行搜索检测

5. Botnets 僵尸网络
    - Detecting Botnet

6. SPAM