第17章作业参考解答

1、简要分析计算机病毒、木马、蠕虫的区别。

答：

|  |  |  |  |
| --- | --- | --- | --- |
| 比较项目 | 病毒 | 蠕虫 | 木马 |
| 存在形式 | 代码片段 | 独立个体 | 独立个体 |
| 复制机制 | 插入宿主程序 | 自身的复制 | 自身的复制 |
| 传染机制 | 宿主的运行 | 系统存在的网络安全漏洞 | 主动或被动植入目标计算机 |
| 攻击目标 | 本地文件 | 网络上的计算机 | 本地文件和系统、网络上的计算机 |
| 计算机使用者角色 | 病毒传播的关键环节 | 无关（通过程序自身） | 木马传播的关键环节 |
| 防治措施 | 从宿主文件中清除 | 为系统打补丁（Patch） | 停止并删除木马服务程序 |

2、为了提高隐蔽性，木马有哪些隐藏技术？

答：主要有存储隐藏、进程隐藏和通信隐藏。

木马在存储时的隐藏技术主要有：

1）已知文件类型的扩展名。

2）利用文件的“隐藏”属性进行隐藏。

3）木马可以利用系统中的一些特定文件夹（如回收站、控制面板等）实现自身的隐藏。

木马的进程隐藏技术主要有：

1）进程列表欺骗（在任务栏中隐藏或在任务管理器中隐藏）。

2）不使用进程，包括：Rundll32 xxx.dll方式；特洛伊DLL；动态嵌入技术，包括：窗口Hook；挂接API；远程线程注入。

木马的通信隐藏技术主要有：

1）使用ICMP协议进行通信。

2）端口复用。

3、比较分析木马静态检测和动态检测技术的优缺点。

答：静态特征码检测技术的主要优点是简单、检测速度快、准确率高，不足之处在于：不能检测未知恶意软件，对于恶意代码变体的容忍度也很低，稍微变形便无法识别；用户需要不断地升级（离线或在线）杀毒软件特征库，同时随着特征库越来越大，检测的效率会越来越低。

动态检测技术能够检测未知恶意代码、恶意代码的变种，但也存在着不足，如产生的误报率较高，且不能识别出病毒的名称和类型等。因此，现在很多杀毒软件在检测到异常时，例如检测到应用修改Windows注册表、一个进程在进行线程插入等，会给用户弹出告警提示，由用户确定是否允许操作继续，而采用特征码检测技术时，杀毒软件一般在检测到匹配的恶意代码时会默认将其查杀或隔离。