


蠕虫也是一种病毒，因此具有病毒的共同特征。一般的病毒是需要寄生的，它可以通过自己指令的执行，将自己的指令代码写到其他程序的体内，而被感染的文件就被称为“宿主”，例如，Windows下可执行文件的格式为PE格式(Portable Executable)，当需要感染pe文件时，在宿主程序中，建立一个新段，将病毒代码写到新段中，修改的程序入口点等，这样，宿主程序执行的时候，就可以先执行病毒程序，病毒程序运行完之后，在把控制权交给宿主原来的程序指令。

不同病毒主要是感染文件，当然也还有像DIRII这种链接型病毒，还有引导区病毒。引导区病毒他是感染磁盘的引导区，如果是软盘、U盘（闪存盘）、移动硬盘等被感染，这张受感染的盘用在其他机器上后，同样也会感染其他机器，所以传播方式也可以是移动存储设备。蠕虫病毒蠕虫一般不采取利用PE格式插入文件的方法，而是复制自身在互联网环境下进行传播，病毒的传染能力主要是针对计算机内的文件系统而言，而蠕虫病毒的传染目标是互联网内的所有计算机，局域网条件下的共享文件夹，电子邮件Email，网络中的恶意网页，大量存在着漏洞的服务器等都成为蠕虫传播的良好途径。

蠕虫是一种可以独立运行，能主动寻找感染目标并且能够自动传播的恶意程序。蠕虫的传播依赖于特定的计算机漏洞。系统打补丁只能防蠕虫攻击而不能防止计算机病毒攻击。



比较项	传统病毒	蠕虫
存在形式	寄生文件	独立程序
传染机制	宿主程序运行	主动攻击
传染对象	本地文件 或磁盘	(网络中的) 计算机

病毒（包含蠕虫）的共同特征是自我复制、传播、破坏电脑文件，对电脑造成数据上不可逆转的损坏。蠕虫能够利用系统漏洞通过网络进行自我传播的恶意程序，入侵对象是整个互联网上的电脑。它不需要附着在其他程序上，而是独立存在的。当形成规模、传播速度过快时会极大地消耗网络资源导致大面积网络拥塞甚至瘫痪（如，D、S攻击）。

木马独有特征是伪装成正常应用骗取用户信任而入侵，潜伏在电脑中盗取用户资料与信息。木马通过特定的程序来控制另一台计算机。

计算机病毒的特征

- 非授权可执行性
- 隐蔽性
- 传染性
- 潜伏性
- 破坏性
- 可触发性

XXS 攻击 联系和复制
SQL
防火墙

④

→ 恶意代码

① 计算机病毒

② 蠕虫

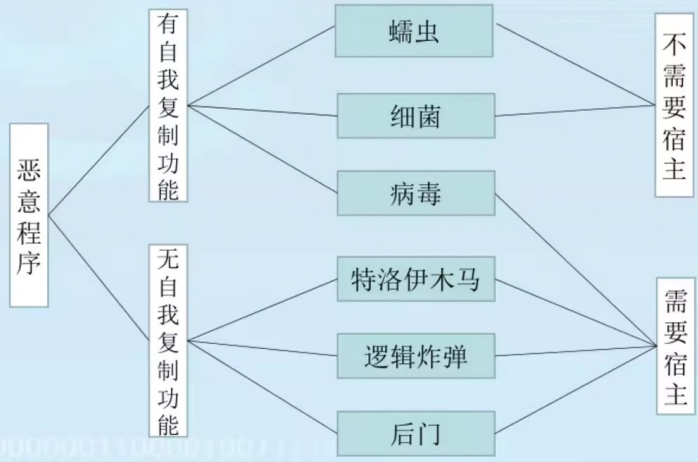
③ 木马

④ Botnet

2种型病毒: 感染可执行的 exe → 宿主
引导型病毒: 感染磁盘
宏病毒: 感染 word
office { excel
ppt

	计算机病毒	特洛伊木马	蠕虫
自我复制性	存在	不存在	存在
感染性	有感染性	无感染性	有感染性
需要宿主	需要	需要	不需要
传染速度	慢	最慢	快
传播路径	感染文件或扇区，通过文件交换或共享传播	通过附加到电子邮件的合法电子邮件和文件传播	直接通过网络传播，包括因特网和内网
传播是否需要用户交互	需要用户交互，如打开程序或文档	需要用户交互，点如点击下载文件或打开附件	一般不需要用户交互，利用目标系统的漏洞或错误配置进行传播
存在形式	寄生	独立程序	独立程序
防范方法	从宿主文件中清除	清除启动项好木马服务程序	更新安全补丁

恶意代码所寄生的**合法程序**被称做载体，也称为宿主程序。



恶意代码类型	定义	特点
计算机病毒	指编制或者在 计算机程序中插入的破坏 计算机功能或者 毁坏数据 ，影响计算机使用，并能 自我复制 的一组计算机指令或者程序代码。	潜伏、传染和破坏
蠕虫	指通过计算机网络 自我复制 ，消耗系统资源和网络资源的程序	扫描、攻击和扩散
特洛伊木马	指一种与远程计算机建立连接，使远程计算机能够通过网络 控制 本地计算机的程序。	欺骗、隐蔽和信息窃取
后门程序	指 绕过 安全性控制而获取对程序或系统访问权的程序方法	隐蔽、不易查杀
逻辑炸弹	指一段 嵌入 计算机系统程序的，通过特殊的数据或时间作为条件 触发 ，试图完成一定 破坏 功能的程序。	潜伏和破坏
病菌	指 不依赖于系统软件 ，能够 自我复制和传播 ，以消耗系统资源为目的的程序。	传染和拒绝服务
用户级 RootKit	指通过替代或者 修改 被系统管理员或普通用户执行的程序进入系统，从而实现 隐藏 和 创建后门 的程序。	隐蔽、潜伏
核心级	指 嵌入 操作系统内核进行 隐藏 和 创建后门 的程序	隐蔽、潜伏

区别与联系

- 计算机病毒是恶意代码，能破坏和删除文件或自我复制；
- 木马是控制程序，黑客通过木马植入控制电脑进行操作，如盗号等

计算机病毒	特洛伊木马
恶意代码。破坏文件。自我复制	控制程序。控制电脑进行操作
直接威胁电脑安全，产生危害	以控制为主，协助破坏
具有感染性（ 最大区别 ）	不具有感染性

➤最大的区别就是病毒具有感染性，而木马一般不具有感染性。