恶意软件

- 定义：恶意软件是指任何的程序或可执行代码，其目的是在用户未授权的情况下更改或控制计算机及网络系统。

分类

1. 独立与寄生的恶意软件
    - 根据其代码是否独立， 可以将其分成独立的和寄生的恶意软件 。
    - 独立的恶意代码能够独立传播和运行，是一个完整的程序，它不需要寄宿在另一个程序中。如蠕虫、木马和僵尸。
    - 非独立的恶意代码只是一段代码，必须寄生在某个程序(或文档)中，作为该程序的一部分进行传播和运行。如病毒。
2. 广义病毒与普通的恶意代码
    - 根据恶意软件是否能自我复制(自动传染) ， 可以将其分成广义病毒及普通的恶意代码。
    - 对于非独立恶意代码，自我复制过程就是将自身嵌入宿主程序的过程，这个过程也称为感染宿主程序的过程。如狭义病毒。
    - 对于独立恶意代码，自我复制过程就是将自身传播给其他系统的过程。如蠕虫。不具有自我复制能力的恶意代码必须借助其他媒介进行传播。如木马和垃圾邮件。

原因

1. 内因：系统和应用软件存在漏洞

   环节方法：软件安全性测试（静态的代码安全测试、动态的渗透测试和程序数据扫描（在内存中进行测试））
2. 外因：利益驱使

恶意软件介绍

后门

后门也被称为陷阱，它是某个正常程序的秘密入口，通过该入口启动程序，可以绕过正常的访问控制过程。因此，获悉后门的人员可以绕过访问控制过程，直接对资源进行访问。

后门最初的作用是程序员开发具有鉴别或登录过程的应用程序时，为避免每一次调试程序时都需输入大量鉴别或登录过程所需要的信息，通过后门启动程序的方式来绕过鉴别或登录过程。当程序正式发布时，程序员会删除该后门。后来程序员有意在程序中留下后门，以防止非授权用户的盗用。再后来，某些（尤其是免费的共享）软件故意留下后门，以窃取目标系统的敏感信息。

逻辑炸弹

逻辑炸弹是包含在正常应用程序中的一段恶意代码，当某种条件出现，如到达某个特定日期、增加或删除某个特定文件等，将触发这一段恶意代码，执行这一段恶意代码将导致非常严重的后果，如删除系统中的重要文件和数据、使系统崩溃等。

间谍软件

间谍软件（Spyware）与商业软件产品有关。有些商业软件产品在安装到用户机器上的时候，未经用户授权就通过Internet连接，让用户方软件与开发商软件进行通信，这部分通信软件就叫做谍件。用户只有安装了基于主机的防火墙，通过记录网络活动，才可能发现软件产品与其开发商在进行定期通讯。

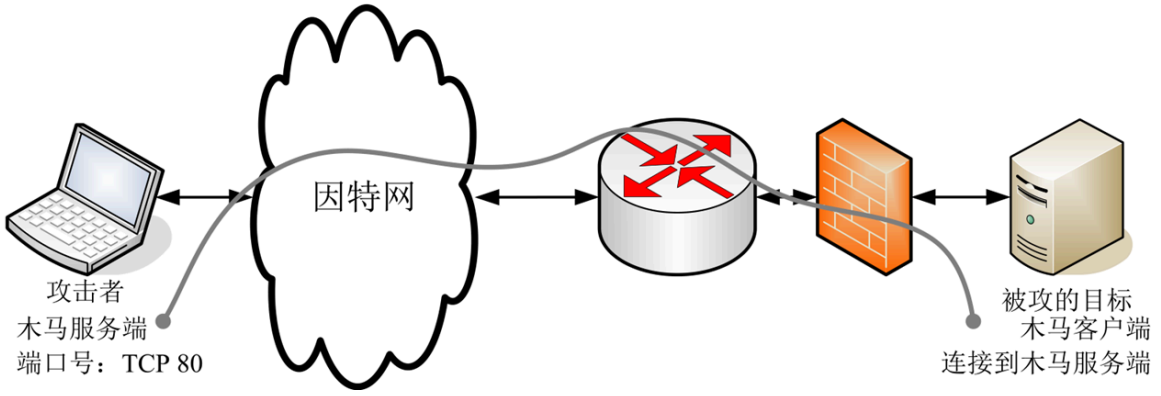
特洛伊木马

特洛伊木马也是包含在正常应用程序中的一段恶意代码，一旦执行这样的应用程序，将触发恶意代码。木马的功能主要在于削弱系统的安全控制机制，尤其是访问控制机制。

一个完整的特洛伊木马套装程序含了两部分：服务端（服务器部分）和客户端（控制器部分）。植入对方电脑的是服务端，而黑客正是利用客户端进入运行了服务端的电脑。运行了木马程序的服务端以后，会产生一个有着容易迷惑用户的名称的进程，暗中打开端口，向指定地点发送数据（如网络游戏的密码，即时通信软件密码和用户上网密码等），黑客甚至可以利用这些打开的端口进入电脑系统。

由于现在的网络信息系统会网络边界配置防火墙以阻止非授权端口被外网连接，使得传统的木马服务端无非被控制，现代的目标主要采用反弹端口的形式：即客户端被植入到目标系统，而服务端在攻击者的电脑中运行，木马客户端运行后主动连接服务端，而由内网到外网的连接是不会被防火墙封堵的。这种木马就是所谓的“反弹端口型木马”。

如图所示的木马服务端开设的端口号为TCP 80，即Web服务的默认端口。木马客户端连接该端口时被防火墙认为是访问 Web服务器，因此允许该连接的数据包通过。



僵尸

Zombie(俗称僵尸)是一种在被入侵者控制的系统上安装的、能对某个特定系统发动攻击的恶意代码。

Zombie主要用于定义恶意代码的功能，并没有涉及该恶意代码的结构和自我复制过程，因此，分别存在符合狭义病毒的定义和蠕虫定义的Zombie。

病毒（重点）

这里的病毒是狭义病毒，即传统意义上的病毒，指那种既具有自我复制能力，又必须寄生在其他程序(或文件)中的恶意代码。

它和陷阱门、逻辑炸弹的最大不同在于自我复制能力。通常情况下，陷阱门、逻辑炸弹不会感染其他实用程序，而病毒会自动将自身添加到其他实用程序中。

结构

病毒的结构包括引导模块、感染模块、触发模块和破坏模块。

- 引导模块：引导模块是病毒的入口模块，它最先获得系统的控制权。引导模块首先将病毒代码引导到内存中的适当位置，其次调用感染模块进行感染，然后根据触发模块的返回值决定是调用病毒的破坏模块还是执行正常的程序。
- 感染模块：感染模块负责完成病毒的感染功能，这是病毒最核心、最关键的代码，需要极高的技术才能设计出来。它寻找要感染的目标文件，判断该文件是否已经被感染了（通过判断该文件是否被标上了感染标志）。如果没有被感染，则进行感染，并标上感染标志。
- 触发模块：触发模块对预先设定的条件进行判断，如果满足则返回真值，否则返回假值。触发的判断条件通常是时间、记数、特定事件、特定程序执行等。
- 破坏模块：破坏模块完成具体的破坏作用，其破坏形式和表象由病毒编写者的目的决定。

蠕虫（重点）

蠕虫也是一种病毒，但它和狭义病毒的最大不同在于自我复制过程。病毒的自我复制过程需要人工干预，无论是运行感染病毒的实用程序，还是打开包含宏病毒的电子邮件，都不是由病毒程序自我完成的。蠕虫的传播不需要人工干预，他其实是能完成特殊攻击过程的自治软件，它自动完成以下任务：

① 查找攻击对象：利用网络侦察技术查找下一个存在漏洞的目标。

② 入侵目标：利用漏洞入侵目标系统。

③ 复制自己：复制自己到被攻击的系统，并运行它。

传播机制

(1)利用系统漏洞主动传播

(2)利用电子邮件系统传播

(3)通过局域网传播

(4)通过即时工具传播

(5)多种方式组合传播

防御方法

① 基于签名的蠕虫扫描过滤

② 基于过滤的蠕虫控制

③ 基于有效载荷分类的蠕虫控制

④ 阈值随机游走扫描检测

⑤ 速率限制和速率停止

狭义病毒和蠕虫的区别

区别	狭义病毒	蠕虫
存在形式	是寄生体	是独立体
复制形式	插入宿主文件	自身进行复制

区别	狭义病毒	蠕虫
传染机制	利用宿主程序运行	利用系统漏洞
触发传染	由计算机使用者触发	程序自身触发
攻击目标	攻击本地文件	攻击网络其他计算机
影响重点	主要影响文件系统	主要影响网络性能和系统性能