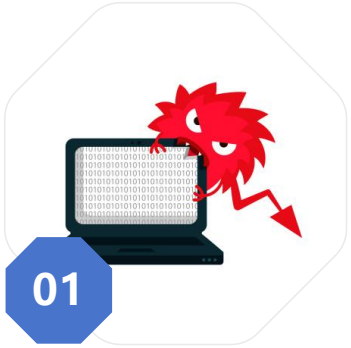
第3章 病毒的基本概念、原理和分类

计算机感染病毒的典型现象

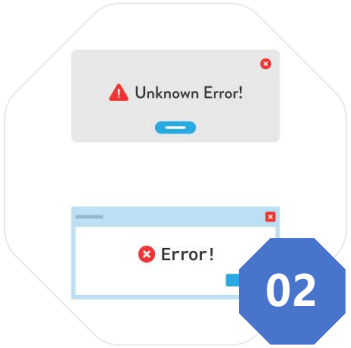
系统性能下降

计算机感染病毒后，系统资源被非法占用，导致运行速度变慢，处理任务的效率显著下降。



异常弹窗与消息

用户可能会频繁遇到不请自来的广告弹窗或错误消息，这些往往是病毒活动的迹象。



程序无法正常运行

病毒可能会破坏或修改程序文件，导致用户在尝试打开或运行应用程序时遇到困难。

病毒传播的途径

电子邮件附件

通过含有恶意代码的电子邮件附件，用户在打开或下载附件时，病毒便有机会感染计算机。

网络下载与共享

从互联网下载的软件或文件，尤其是来自不可靠来源的，可能包含病毒，共享网络资源时也可能传播病毒。

移动存储设备

使用USB驱动器、外部硬盘等移动存储设备在不同计算机间传输数据时，未受保护的设备可能成为病毒传播的媒介。

病毒对系统文件的影响

文件损坏或丢失

病毒可能会损坏或删除系统文件和用户数据文件，导致重要信息丢失。

系统配置被篡改

病毒可能修改系统设置，如注册表项，从而影响计算机的正常运行。

隐私信息泄露

某些病毒设计用于窃取用户的个人信息，如登录凭证、财务数据等，并将其发送给攻击者。

病毒对网络的影响

网络流量异常

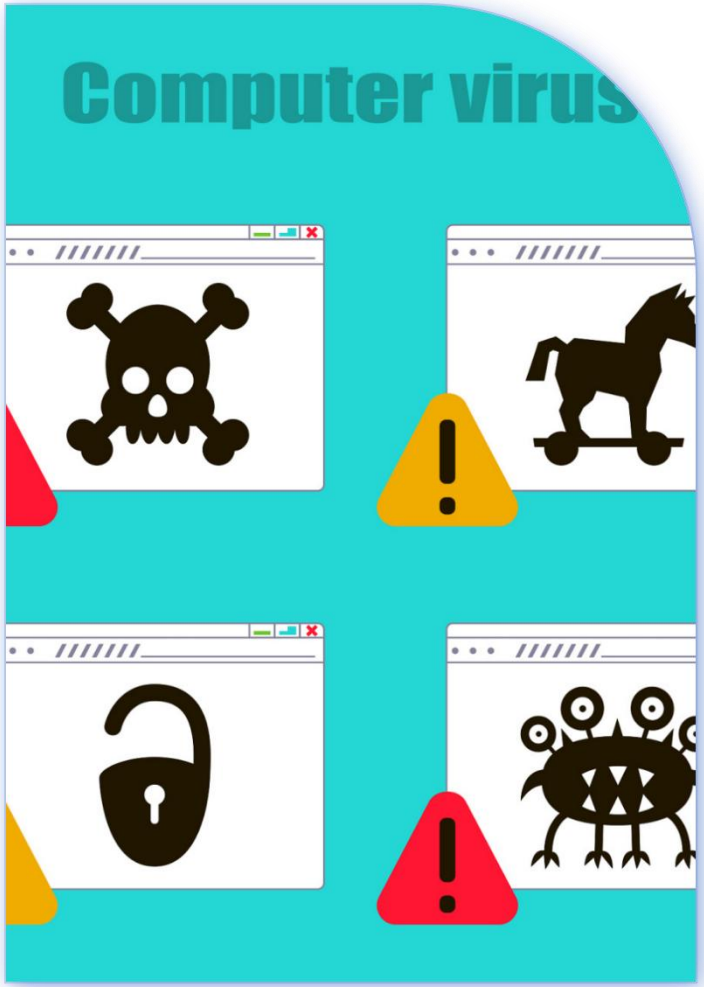
感染病毒的计算机可能会被利用来发起或参与网络攻击，导致网络流量异常增加。

服务中断与拒绝

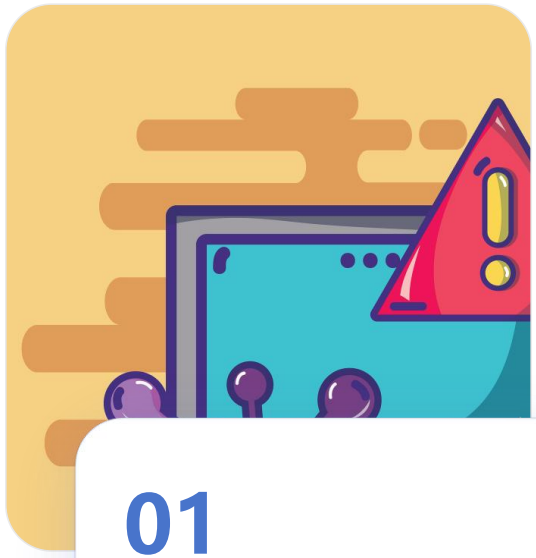
病毒可能通过分布式拒绝服务(DDoS)攻击使网络服务中断，影响网络的可用性。

分布式拒绝服务攻击

病毒可以将被感染的计算机变成“僵尸网络”，用于发起大规模的DDoS攻击，瘫痪目标服务器。



病毒的自我复制机制



01

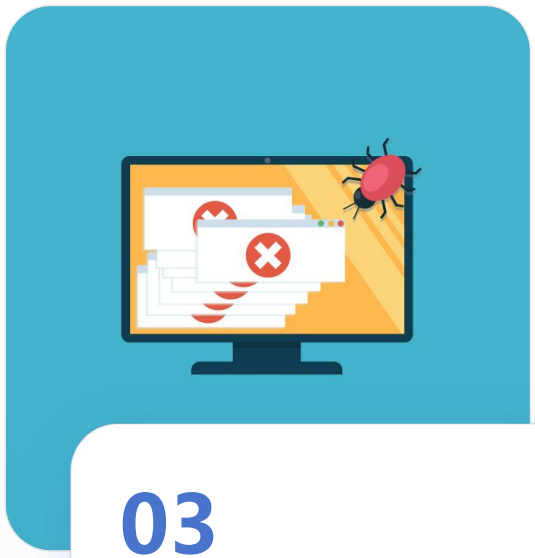
引导区感染

病毒可以感染计算机的引导区，当系统启动时自动加载病毒代码，从而实现自我复制。

02

文件感染

病毒通过感染可执行文件，当这些文件被运行时，病毒代码被执行并传播。



03

宏病毒

宏病毒利用应用程序（如Microsoft Office）中的宏功能来传播，当文档被打开时激活。

病毒的隐蔽技术

01

加壳与加密

病毒作者使用加壳工具对病毒进行加密和压缩，以逃避杀毒软件的检测。

02

多态病毒

多态病毒能够改变自己的代码结构，每次感染时都呈现不同的形态，使得识别和清除变得更加困难。

03

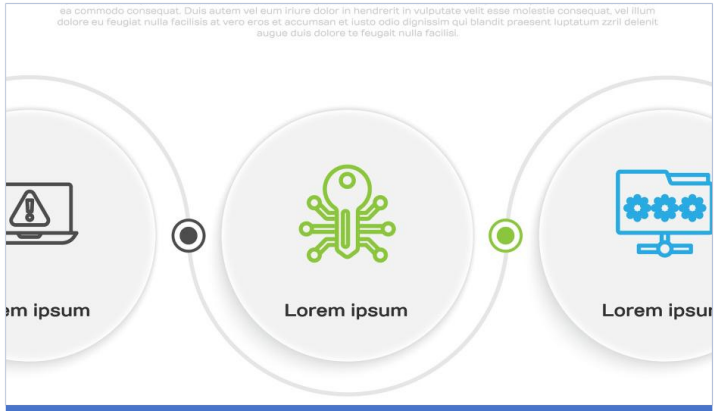
隐写术

病毒使用隐写术隐藏其代码，通常嵌入到正常文件中，使得检测变得复杂。

病毒的触发机制

定时触发

某些病毒被设计为在特定时间或日期自动激活，执行其破坏性行为。



事件触发

病毒可能在特定的系统事件发生时触发，例如系统启动、用户登录等。

用户行为触发

用户的某些行为，如打开特定文件、点击链接等，可能激活病毒。

病毒的破坏行为

数据破坏

病毒可能会删除或损坏文件，导致用户数据丢失或系统文件损坏。

系统瘫痪

某些病毒设计目的是使整个计算机系统瘫痪，导致用户无法使用计算机。

资源占用

病毒可能会占用大量系统资源，如CPU和内存，影响计算机的正常运行。

防范病毒的策略与措施

01

安装防病毒软件

安装并定期更新防病毒软件是预防病毒的第一道防线，可以检测并清除病毒威胁。

02

定期更新系统与软件

及时更新操作系统和应用程序可以修补安全漏洞，减少病毒利用这些漏洞进行攻击的机会。

03

安全上网习惯

培养良好的上网习惯，如不随意点击不明链接、不下载不明来源的文件，可以有效降低感染病毒的风险。