# 计算机病毒

[锁定](https://baike.baidu.com/view/10812319.htm" \o "锁定" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)

本词条由[“科普中国”科学百科词条编写与应用工作项目](https://baike.baidu.com/science" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank) 审核 。

计算机病毒*（Computer Virus）*是编制者在计算机程序中插入的破坏计算机功能或者数据的代码，能影响计算机使用，能自我复制的一组[计算机](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)指令或者程序[代码](https://baike.baidu.com/item/%E4%BB%A3%E7%A0%81/86048" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)。

计算机病毒具有传播性、隐蔽性、感染性、潜伏性、可激发性、表现性或破坏性。计算机病毒的生命周期：开发期→传染期→潜伏期→发作期→发现期→消化期→消亡期。

计算机病毒是一个程序，一段可执行码。就像生物病毒一样，具有自我繁殖、互相传染以及激活再生等生物病毒特征。计算机病毒有独特的复制能力，它们能够快速蔓延，又常常难以根除。它们能把自身附着在各种类型的文件上，当文件被复制或从一个用户传送到另一个用户时，它们就随同文件一起蔓延开来。

**中文名**

计算机病毒

**外文名**

Computer Virus

**诞生年代**

20世纪

**危害最大**

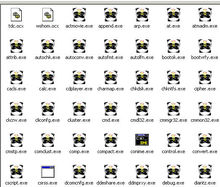
CIH [1]

## 目录

1. 1 [定义](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/174112?fr=aladdin" \l "1)
2. 2 [发展](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/174112?fr=aladdin" \l "2)
3. ▪ [科幻小说](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/174112?fr=aladdin" \l "2_1)
4. ▪ [病毒程序](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/174112?fr=aladdin" \l "2_2)
5. 3 [特征](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/174112?fr=aladdin" \l "3)
6. 4 [原理](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/174112?fr=aladdin" \l "4)
7. 5 [感染策略](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/174112?fr=aladdin" \l "5)
8. ▪ [非常驻型病毒](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/174112?fr=aladdin" \l "5_1)
9. ▪ [常驻型病毒](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/174112?fr=aladdin" \l "5_2)
10. 6 [分类](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/174112?fr=aladdin" \l "6)
11. 7 [命名](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/174112?fr=aladdin" \l "7)
12. 8 [征兆预防](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/174112?fr=aladdin" \l "8)
13. ▪ [病毒征兆](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/174112?fr=aladdin" \l "8_1)
14. ▪ [保护预防](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/174112?fr=aladdin" \l "8_2)
15. 9 [免杀技术以及新特征](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/174112?fr=aladdin" \l "9)

## 定义

[计算机](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)病毒*（Computer Virus）*在

[](https://baike.baidu.com/pic/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/174112/0/09fa513d269759ee9ab32ad0bffb43166c22dfce?fr=lemma%26ct=single)熊猫烧香病毒（尼姆亚病毒变种） [2]

《*[中华人民共和国计算机信息系统安全保护条例](https://baike.baidu.com/item/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E8%AE%A1%E7%AE%97%E6%9C%BA%E4%BF%A1%E6%81%AF%E7%B3%BB%E7%BB%9F%E5%AE%89%E5%85%A8%E4%BF%9D%E6%8A%A4%E6%9D%A1%E4%BE%8B" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)*》中被明确定义，病毒指“[编制](https://baike.baidu.com/item/%E7%BC%96%E5%88%B6" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)者在[计算机程序](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%A8%8B%E5%BA%8F" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)中插入的破坏计算机[功能](https://baike.baidu.com/item/%E5%8A%9F%E8%83%BD" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)或者破坏[数据](https://baike.baidu.com/item/%E6%95%B0%E6%8D%AE/5947370" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)，[影响](https://baike.baidu.com/item/%E5%BD%B1%E5%93%8D/2083" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)计算机使用并且能够自我[复制](https://baike.baidu.com/item/%E5%A4%8D%E5%88%B6/33067" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)的一组计算机[指令](https://baike.baidu.com/item/%E6%8C%87%E4%BB%A4" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)或者程序代码”。 [3]

计算机病毒与[医学](https://baike.baidu.com/item/%E5%8C%BB%E5%AD%A6" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)上的“[病毒](https://baike.baidu.com/item/%E7%97%85%E6%AF%92" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)”不同，计算机病毒不是[天然](https://baike.baidu.com/item/%E5%A4%A9%E7%84%B6/84419" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)存在的，是人[利用](https://baike.baidu.com/item/%E5%88%A9%E7%94%A8" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)计算机[软件](https://baike.baidu.com/item/%E8%BD%AF%E4%BB%B6/12053" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)和[硬件](https://baike.baidu.com/item/%E7%A1%AC%E4%BB%B6" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)所固有的[脆弱性](https://baike.baidu.com/item/%E8%84%86%E5%BC%B1%E6%80%A7" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)编制的一组[指令](https://baike.baidu.com/item/%E6%8C%87%E4%BB%A4" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)集或程序代码。它能[潜伏](https://baike.baidu.com/item/%E6%BD%9C%E4%BC%8F/7704875" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)在计算机的[存储介质](https://baike.baidu.com/item/%E5%AD%98%E5%82%A8%E4%BB%8B%E8%B4%A8" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)（或程序）里，条件[满足](https://baike.baidu.com/item/%E6%BB%A1%E8%B6%B3/33336" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)时即被[激活](https://baike.baidu.com/item/%E6%BF%80%E6%B4%BB" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)，通过修改其他[程序](https://baike.baidu.com/item/%E7%A8%8B%E5%BA%8F/13831935" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)的方法将自己的精确[拷贝](https://baike.baidu.com/item/%E6%8B%B7%E8%B4%9D" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)或者可能[演化](https://baike.baidu.com/item/%E6%BC%94%E5%8C%96" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)的形式放入其他[程序](https://baike.baidu.com/item/%E7%A8%8B%E5%BA%8F/13831935" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)中。从而[感染](https://baike.baidu.com/item/%E6%84%9F%E6%9F%93/44330" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)其他程序，对[计算机](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)资源进行破坏，所谓的病毒就是人为造成的，对其他[用户](https://baike.baidu.com/item/%E7%94%A8%E6%88%B7" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)的[危害](https://baike.baidu.com/item/%E5%8D%B1%E5%AE%B3" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)[性](https://baike.baidu.com/item/%E6%80%A7" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)很大。 [4-6]

## 发展

第一份关于计算机病毒[理论](https://baike.baidu.com/item/%E7%90%86%E8%AE%BA/1732500" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)的[学术](https://baike.baidu.com/item/%E5%AD%A6%E6%9C%AF" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)工作（ "病毒" 一词当时并未使用）于 1949 年由[约翰·冯·诺伊曼](https://baike.baidu.com/item/%E7%BA%A6%E7%BF%B0%C2%B7%E5%86%AF%C2%B7%E8%AF%BA%E4%BC%8A%E6%9B%BC" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)完成。以 "*Theory and Organization of Complicated Automata*" 为题的一场在[伊利诺伊大学](https://baike.baidu.com/item/%E4%BC%8A%E5%88%A9%E8%AF%BA%E4%BC%8A%E5%A4%A7%E5%AD%A6" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)的演讲，后改以 "Theory of self-reproducing automata" 为题出版。冯·[诺伊曼](https://baike.baidu.com/item/%E8%AF%BA%E4%BC%8A%E6%9B%BC/4616623" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)在他的论文中[描述](https://baike.baidu.com/item/%E6%8F%8F%E8%BF%B0" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)一个计算机程序如何复制其自身。

1980 年，Jürgen Kraus 于[多特蒙德大学](https://baike.baidu.com/item/%E5%A4%9A%E7%89%B9%E8%92%99%E5%BE%B7%E5%A4%A7%E5%AD%A6" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)撰写他的学位论文 "Self-reproduction of programs"。论文中假设计算机程序可以表现出如同[病毒](https://baike.baidu.com/item/%E7%97%85%E6%AF%92" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)般的行为。

“病毒”一词最早用来表达此意是在[弗雷德·科恩](https://baike.baidu.com/item/%E5%BC%97%E9%9B%B7%E5%BE%B7%C2%B7%E7%A7%91%E6%81%A9" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)*（Fred Cohen）*1984年的论文《电脑病毒实验》。 [7]

1983 年 11月，在一次[国际](https://baike.baidu.com/item/%E5%9B%BD%E9%99%85" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)计算机[安全](https://baike.baidu.com/item/%E5%AE%89%E5%85%A8/32778" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)学术[会议](https://baike.baidu.com/item/%E4%BC%9A%E8%AE%AE" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)上，[美国](https://baike.baidu.com/item/%E7%BE%8E%E5%9B%BD/125486" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)学者[科恩](https://baike.baidu.com/item/%E7%A7%91%E6%81%A9/3562355" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)第一次明确提出计算机病毒的[概念](https://baike.baidu.com/item/%E6%A6%82%E5%BF%B5" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)，并进行了[演示](https://baike.baidu.com/item/%E6%BC%94%E7%A4%BA" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)。

1986年年初，巴基斯坦兄弟编写了“[大脑](https://baike.baidu.com/item/%E5%A4%A7%E8%84%91" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)（*[Brain](https://baike.baidu.com/item/Brain" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)*）”病毒，又被称为“[巴基斯坦](https://baike.baidu.com/item/%E5%B7%B4%E5%9F%BA%E6%96%AF%E5%9D%A6" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)”病毒。

1987年，第一个电脑病毒C-BRAIN诞生。由[巴基斯坦](https://baike.baidu.com/item/%E5%B7%B4%E5%9F%BA%E6%96%AF%E5%9D%A6" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)兄弟：巴斯特（*Basit*）和阿姆捷特（*Amjad*）编写。计算机病毒主要是[引导型病毒](https://baike.baidu.com/item/%E5%BC%95%E5%AF%BC%E5%9E%8B%E7%97%85%E6%AF%92" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)，具有代表性的是“[小球](https://baike.baidu.com/item/%E5%B0%8F%E7%90%83" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)”和“[石头](https://baike.baidu.com/item/%E7%9F%B3%E5%A4%B4/805" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)”病毒。

1988年在[财政部](https://baike.baidu.com/item/%E8%B4%A2%E6%94%BF%E9%83%A8" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)的计算机上发现的，[中国](https://baike.baidu.com/item/%E4%B8%AD%E5%9B%BD/1122445" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)最早的计算机病毒。

1989年，引导型病毒发展为可以感染[硬盘](https://baike.baidu.com/item/%E7%A1%AC%E7%9B%98" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)，[典型](https://baike.baidu.com/item/%E5%85%B8%E5%9E%8B" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)的[代表](https://baike.baidu.com/item/%E4%BB%A3%E8%A1%A8" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)有“石头2”。

1990年，发展为[复合型病毒](https://baike.baidu.com/item/%E5%A4%8D%E5%90%88%E5%9E%8B%E7%97%85%E6%AF%92" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)，可感染[COM](https://baike.baidu.com/item/COM/5596" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)和[EXE](https://baike.baidu.com/item/EXE" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)文件。

1992年，利用[DOS](https://baike.baidu.com/item/DOS/32025" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)加载文件的[优先](https://baike.baidu.com/item/%E4%BC%98%E5%85%88" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)顺序进行[工作](https://baike.baidu.com/item/%E5%B7%A5%E4%BD%9C/82254" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)，具有代表性的是“[金蝉](https://baike.baidu.com/item/%E9%87%91%E8%9D%89" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)”病毒。

1995年，当生成器的生成[结果](https://baike.baidu.com/item/%E7%BB%93%E6%9E%9C/29394" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)为病毒时，就产生了这种[复杂](https://baike.baidu.com/item/%E5%A4%8D%E6%9D%82/7270408" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)的“病毒生成器” ，[幽灵](https://baike.baidu.com/item/%E5%B9%BD%E7%81%B5/3149" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)病毒流行中国。 [8]  典型病毒代表是“病毒制造机” “[VCL](https://baike.baidu.com/item/VCL" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)”。

1998年[台湾](https://baike.baidu.com/item/%E5%8F%B0%E6%B9%BE" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)[大同](https://baike.baidu.com/item/%E5%A4%A7%E5%90%8C/9011" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)工学院[学生](https://baike.baidu.com/item/%E5%AD%A6%E7%94%9F/3363" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)陈盈豪编制了[CIH](https://baike.baidu.com/item/CIH" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)病毒。

2000年最具破坏力的10种病毒分别是：Kakworm，[爱虫](https://baike.baidu.com/item/%E7%88%B1%E8%99%AB" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)， Apology-B， Marker ， [Pretty](https://baike.baidu.com/item/Pretty" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank) ，[Stages-A](https://baike.baidu.com/item/Stages-A" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)，Navidad，Ska-Happy99 ，WM97/Thus ，XM97/Jin。 [9]

2003年，中国[大陆](https://baike.baidu.com/item/%E5%A4%A7%E9%99%86/686999" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)地区发作最多的十个病毒，分别是：红色结束符、[爱情后门](https://baike.baidu.com/item/%E7%88%B1%E6%83%85%E5%90%8E%E9%97%A8" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)、FUNLOVE、QQ传送者、冲击波杀手、罗拉、[求职信](https://baike.baidu.com/item/%E6%B1%82%E8%81%8C%E4%BF%A1" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)、尼姆达II、[QQ木马](https://baike.baidu.com/item/QQ%E6%9C%A8%E9%A9%AC" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)、[CIH](https://baike.baidu.com/item/CIH" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)。 [1]  [10]

2005年，1月到10月，[金山](https://baike.baidu.com/item/%E9%87%91%E5%B1%B1/6325074" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)反病毒监测中心共截获或[监测](https://baike.baidu.com/item/%E7%9B%91%E6%B5%8B" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)到的病毒达到50179个，其中[木马](https://baike.baidu.com/item/%E6%9C%A8%E9%A9%AC/530" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)、蠕虫、[黑客病毒](https://baike.baidu.com/item/%E9%BB%91%E5%AE%A2%E7%97%85%E6%AF%92" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)占其中的91%，以盗取[用户](https://baike.baidu.com/item/%E7%94%A8%E6%88%B7" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)有价[账号](https://baike.baidu.com/item/%E8%B4%A6%E5%8F%B7" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)的木马病毒（如[网银](https://baike.baidu.com/item/%E7%BD%91%E9%93%B6" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)、[QQ](https://baike.baidu.com/item/QQ" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)、[网游](https://baike.baidu.com/item/%E7%BD%91%E6%B8%B8" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)）为主，病毒多达2000多种。 [11]

2007年1月，病毒累计感染了[中国](https://baike.baidu.com/item/%E4%B8%AD%E5%9B%BD/1122445" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)80%的[用户](https://baike.baidu.com/item/%E7%94%A8%E6%88%B7" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)，其中78%以上的病毒为木马、后门病毒。 [12]  [熊猫烧香](https://baike.baidu.com/item/%E7%86%8A%E7%8C%AB%E7%83%A7%E9%A6%99" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)肆虐全球。 [13]

2010年，[越南](https://baike.baidu.com/item/%E8%B6%8A%E5%8D%97" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)全国计算机数量已500万台，其中93%受过病毒感染，感染电脑病毒共损失59000万亿[越南盾](https://baike.baidu.com/item/%E8%B6%8A%E5%8D%97%E7%9B%BE" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)。

[6]  [14]

2017年5月，一种名为“想哭”的勒索病毒席卷全球，在短短一周时间里，上百个国家和地区受到影响。据美国有线新闻网报道，截至2017年5月15日，大约有150个国家受到影响，至少30万台电脑被病毒感染。 [15]

### 科幻小说

而病毒一词广为人知是得力于[科幻小说](https://baike.baidu.com/item/%E7%A7%91%E5%B9%BB%E5%B0%8F%E8%AF%B4" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)。一部是1970年代中期大卫·杰洛德（David Gerrold）的《When H.A.R.L.I.E. was One》，描述了一个叫“病毒”的[程序](https://baike.baidu.com/item/%E7%A8%8B%E5%BA%8F/71525" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)和与之对战的叫“[抗体](https://baike.baidu.com/item/%E6%8A%97%E4%BD%93/1210844" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)”的程序；另一部是约翰·布鲁勒尔（John Brunner）1975年的小说《震荡波骑士（ShakewaveRider）》，描述了一个叫做“磁带蠕虫”、在网络上删除数据的程序。 [16]

### 病毒程序

1960年代初，[美国](https://baike.baidu.com/item/%E7%BE%8E%E5%9B%BD/125486" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)[麻省理工学院](https://baike.baidu.com/item/%E9%BA%BB%E7%9C%81%E7%90%86%E5%B7%A5%E5%AD%A6%E9%99%A2" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)的一些青年研究人员，在做完工作后，利用业务时间玩一种他们自己创造的[计算机游戏](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E6%B8%B8%E6%88%8F" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)。做法是某个人编制一段小程序，然后输入到计算机中运行，并销毁对方的游戏程序。而这也可能就是计算机病毒的雏形。 [17]

## 特征

**繁殖性**

计算机病毒可以像[生物](https://baike.baidu.com/item/%E7%94%9F%E7%89%A9/161443" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)[病毒](https://baike.baidu.com/item/%E7%97%85%E6%AF%92" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)一样进行[繁殖](https://baike.baidu.com/item/%E7%B9%81%E6%AE%96/22480" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)，当[正常](https://baike.baidu.com/item/%E6%AD%A3%E5%B8%B8" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)程序[运行](https://baike.baidu.com/item/%E8%BF%90%E8%A1%8C/5480697" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)时，它也进行运行[自身](https://baike.baidu.com/item/%E8%87%AA%E8%BA%AB" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)复制，是否具有繁殖、感染的[特征](https://baike.baidu.com/item/%E7%89%B9%E5%BE%81" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)是[判断](https://baike.baidu.com/item/%E5%88%A4%E6%96%AD/33345" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)某段程序为计算机病毒的首要[条件](https://baike.baidu.com/item/%E6%9D%A1%E4%BB%B6/1783021" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)。

**破坏性**

计算机中毒后，可能会导致[正常](https://baike.baidu.com/item/%E6%AD%A3%E5%B8%B8" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)的程序无法运行，把计算机内的文件[删除](https://baike.baidu.com/item/%E5%88%A0%E9%99%A4/297096" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)或受到不同程度的[损坏](https://baike.baidu.com/item/%E6%8D%9F%E5%9D%8F" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)。破坏引导扇区及[BIOS](https://baike.baidu.com/item/BIOS" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)，硬件[环境](https://baike.baidu.com/item/%E7%8E%AF%E5%A2%83" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)破坏。

**传染性**

计算机病毒传染性是指计算机病毒通过[修改](https://baike.baidu.com/item/%E4%BF%AE%E6%94%B9" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)别的程序将自身的复制品或其变体传染到其它无毒的对象上，这些对象可以是一个程序也可以是[系统](https://baike.baidu.com/item/%E7%B3%BB%E7%BB%9F" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)中的某一个部件。

**潜伏性**

计算机病毒潜伏性是指计算机病毒可以依附于其它媒体[寄生](https://baike.baidu.com/item/%E5%AF%84%E7%94%9F/331673" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)的能力，侵入后的病毒[潜伏](https://baike.baidu.com/item/%E6%BD%9C%E4%BC%8F/7704875" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)到条件[成熟](https://baike.baidu.com/item/%E6%88%90%E7%86%9F/80699" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)才[发作](https://baike.baidu.com/item/%E5%8F%91%E4%BD%9C" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)， 会使电脑[变慢](https://baike.baidu.com/item/%E5%8F%98%E6%85%A2" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)。

**隐蔽性**

计算机病毒具有很强的隐蔽性，可以[通过](https://baike.baidu.com/item/%E9%80%9A%E8%BF%87" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)病毒软件[检查](https://baike.baidu.com/item/%E6%A3%80%E6%9F%A5" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)出来少数，隐蔽性计算机病毒[时隐时现](https://baike.baidu.com/item/%E6%97%B6%E9%9A%90%E6%97%B6%E7%8E%B0" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)、[变化无常](https://baike.baidu.com/item/%E5%8F%98%E5%8C%96%E6%97%A0%E5%B8%B8" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)，这类病毒处理起来非常[困难](https://baike.baidu.com/item/%E5%9B%B0%E9%9A%BE" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)。

**可触发性**

[编制](https://baike.baidu.com/item/%E7%BC%96%E5%88%B6" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)计算机病毒的人，一般都为病毒程序[设定](https://baike.baidu.com/item/%E8%AE%BE%E5%AE%9A" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)了一些触发条件，例如，[系统](https://baike.baidu.com/item/%E7%B3%BB%E7%BB%9F" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)时钟的某个时间或日期、系统运行了某些程序等。一旦[条件](https://baike.baidu.com/item/%E6%9D%A1%E4%BB%B6/1783021" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)满足，计算机病毒就会“[发作](https://baike.baidu.com/item/%E5%8F%91%E4%BD%9C" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)”，使系统遭到破坏。**[18-19]**[20]

## 原理

病毒[依附](https://baike.baidu.com/item/%E4%BE%9D%E9%99%84" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)[存储](https://baike.baidu.com/item/%E5%AD%98%E5%82%A8" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)介质[软盘](https://baike.baidu.com/item/%E8%BD%AF%E7%9B%98" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)、 [硬盘](https://baike.baidu.com/item/%E7%A1%AC%E7%9B%98" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)等构成[传染](https://baike.baidu.com/item/%E4%BC%A0%E6%9F%93/33812" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)源。病毒传染的媒介由工作的[环境](https://baike.baidu.com/item/%E7%8E%AF%E5%A2%83" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)来定。病毒[激活](https://baike.baidu.com/item/%E6%BF%80%E6%B4%BB" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)是将病毒放在内存， 并设置触发条件，触发的[条件](https://baike.baidu.com/item/%E6%9D%A1%E4%BB%B6/1783021" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)是多样化的， 可以是[时钟](https://baike.baidu.com/item/%E6%97%B6%E9%92%9F/69960" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)，系统的日期，用户[标识符](https://baike.baidu.com/item/%E6%A0%87%E8%AF%86%E7%AC%A6" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)，也可以是系统一次[通信](https://baike.baidu.com/item/%E9%80%9A%E4%BF%A1/300982" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)等。条件成熟病毒就[开始](https://baike.baidu.com/item/%E5%BC%80%E5%A7%8B/4782" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)自我复制到传染对象中，进行各种[破坏](https://baike.baidu.com/item/%E7%A0%B4%E5%9D%8F/32871" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)活动等。

病毒的传染是病毒性能的一个重要[标志](https://baike.baidu.com/item/%E6%A0%87%E5%BF%97" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)。在传染环节中，病毒复制一个自身[副本](https://baike.baidu.com/item/%E5%89%AF%E6%9C%AC/3646" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)到传染对象中去。 [21-22]

## 感染策略

为了能够复制其自身，病毒必须能够运行代码并能够对内存运行写操作。基于这个原因，许多病毒都是将自己附着在合法的可执行文件上。如果用户企图运行该可执行文件，那么病毒就有机会运行。病毒可以根据运行时所表现出来的行为分成两类。非常驻型病毒会立即查找其它宿主并伺机加以感染，之后再将控制权交给被感染的应用程序。常驻型病毒被运行时并不会查找其它宿主。相反的，一个常驻型病毒会将自己加载内存并将控制权交给宿主。该病毒于背景中运行并伺机感染其它目标。 [23]

### 非常驻型病毒

非常驻型病毒可以被想成具有搜索模块和复制模块的程序。搜索模块负责查找可被感染的文件，一旦搜索到该文件，搜索模块就会启动复制模块进行感染。 [24]

### 常驻型病毒

常驻型病毒包含复制模块，其角色类似于非常驻型病毒中的复制模块。复制模块在常驻型病毒中不会被搜索模块调用。病毒在被运行时会将复制模块加载内存，并确保当操作系统运行特定动作时，该复制模块会被调用。例如，复制模块会在操作系统运行其它文件时被调用。在这个例子中，所有可以被运行的文件均会被感染。常驻型病毒有时会被区分成快速感染者和慢速感染者。快速感染者会试图感染尽可能多的文件。例如，一个快速感染者可以感染所有被访问到的文件。这会对杀毒软件造成特别的问题。当运行全系统防护时，杀毒软件需要扫描所有可能会被感染的文件。如果杀毒软件没有察觉到内存中有快速感染者，快速感染者可以借此搭便车，利用杀毒软件扫描文件的同时进行感染。快速感染者依赖其快速感染的能力。但这同时会使得快速感染者容易被侦测到，这是因为其行为会使得系统性能降低，进而增加被杀毒软件侦测到的风险。相反的，慢速感染者被设计成偶而才对目标进行感染，如此一来就可避免被侦测到的机会。例如，有些慢速感染者只有在其它文件被拷贝时才会进行感染。但是慢速感染者此种试图避免被侦测到的作法似乎并不成功。 [25]

## 分类

**破坏性**

[良性](https://baike.baidu.com/item/%E8%89%AF%E6%80%A7" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)病毒、恶性病毒、极恶性病毒、[灾难](https://baike.baidu.com/item/%E7%81%BE%E9%9A%BE" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)性病毒。

**传染方式**

引导区型病毒主要通过[软盘](https://baike.baidu.com/item/%E8%BD%AF%E7%9B%98" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)在操作系统中传播，感染引导区，[蔓延](https://baike.baidu.com/item/%E8%94%93%E5%BB%B6/2342" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)到硬盘，并能感染到硬盘中的"主引导[记录](https://baike.baidu.com/item/%E8%AE%B0%E5%BD%95/1837758" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)"。

文件型病毒是文件感染者，也称为“[寄生](https://baike.baidu.com/item/%E5%AF%84%E7%94%9F/331673" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)病毒”。它运行在计算机[存储器](https://baike.baidu.com/item/%E5%AD%98%E5%82%A8%E5%99%A8" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)中，通常感染扩展名为[COM](https://baike.baidu.com/item/COM/5596" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)、[EXE](https://baike.baidu.com/item/EXE" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)、[SYS](https://baike.baidu.com/item/SYS" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)等类型的文件。

混合型病毒具有[引导区](https://baike.baidu.com/item/%E5%BC%95%E5%AF%BC%E5%8C%BA" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)型病毒和[文件](https://baike.baidu.com/item/%E6%96%87%E4%BB%B6" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)型病毒两者的特点。

[宏](https://baike.baidu.com/item/%E5%AE%8F/2648286" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)病毒是指用[BASIC语言](https://baike.baidu.com/item/BASIC%E8%AF%AD%E8%A8%80" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)编写的病毒程序寄存在[Office](https://baike.baidu.com/item/Office/6834573" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)文档上的宏代码。宏病毒影响对文档的各种[操作](https://baike.baidu.com/item/%E6%93%8D%E4%BD%9C/33052" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)。

**连接方式**

[源码](https://baike.baidu.com/item/%E6%BA%90%E7%A0%81" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)型病毒攻击[高级语言](https://baike.baidu.com/item/%E9%AB%98%E7%BA%A7%E8%AF%AD%E8%A8%80" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)编写的源程序，在源程序[编译](https://baike.baidu.com/item/%E7%BC%96%E8%AF%91" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)之前插入[其中](https://baike.baidu.com/item/%E5%85%B6%E4%B8%AD" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)，并随源程序一起编译、[连接](https://baike.baidu.com/item/%E8%BF%9E%E6%8E%A5/70199" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)成可执行文件。源码型病毒较为少见，亦[难以](https://baike.baidu.com/item/%E9%9A%BE%E4%BB%A5" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)编写。

入侵型病毒可用自身[代替](https://baike.baidu.com/item/%E4%BB%A3%E6%9B%BF" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)正常程序中的部分[模块](https://baike.baidu.com/item/%E6%A8%A1%E5%9D%97" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)或[堆栈](https://baike.baidu.com/item/%E5%A0%86%E6%A0%88" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)区。因此这类病毒只攻击某些[特定](https://baike.baidu.com/item/%E7%89%B9%E5%AE%9A" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)程序，针对性强。一般情况下也难以被[发现](https://baike.baidu.com/item/%E5%8F%91%E7%8E%B0/75066" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)，清除起来也较[困难](https://baike.baidu.com/item/%E5%9B%B0%E9%9A%BE" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)。

操作系统型病毒可用其[自身](https://baike.baidu.com/item/%E8%87%AA%E8%BA%AB" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)部分加入或[替代](https://baike.baidu.com/item/%E6%9B%BF%E4%BB%A3" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)操作系统的部分[功能](https://baike.baidu.com/item/%E5%8A%9F%E8%83%BD" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)。因其直接感染操作系统，这类病毒的危害性也较大。

外壳型病毒[通常](https://baike.baidu.com/item/%E9%80%9A%E5%B8%B8" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)将自身附在[正常](https://baike.baidu.com/item/%E6%AD%A3%E5%B8%B8" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)程序的[开头](https://baike.baidu.com/item/%E5%BC%80%E5%A4%B4" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)或[结尾](https://baike.baidu.com/item/%E7%BB%93%E5%B0%BE" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)，相当于给正常程序加了个[外壳](https://baike.baidu.com/item/%E5%A4%96%E5%A3%B3/4765104" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)。大部份的文件型病毒都属于这一类。 [26]

计算机病毒种类繁多而且复杂，按照不同的方式以及计算机病毒的特点及特性，可以有多种不同的分类方法。同时，根据不同的分类方法，同一种计算机病毒也可以属于不同的计算机病毒种类。

按照计算机病毒属性的方法进行分类，计算机病毒可以根据下面的属性进行分类。

根据病毒存在的媒体划分：

网络病毒——通过计算机网络传播感染网络中的可执行文件。

文件病毒——感染计算机中的文件（如：COM，EXE，DOC等）。

引导型病毒——感染启动扇区（Boot）和硬盘的系统引导扇区（MBR）。

还有这三种情况的混合型，例如：多型病毒（文件和引导型）感染文件和引导扇区两种目标，这样的病毒通常都具有复杂的算法，它们使用非常规的办法侵入系统，同时使用了加密和变形算法。

根据病毒传染渠道划分：

驻留型病毒——这种病毒感染计算机后，把自身的内存驻留部分放在内存（RAM）中，这一部分程序挂接系统调用并合并到操作系统中去，它处于激活状态，一直到关机或重新启动

非驻留型病毒——这种病毒在得到机会激活时并不感染计算机内存，一些病毒在内存中留有小部分，但是并不通过这一部分进行传染，这类病毒也被划分为非驻留型病毒。

根据破坏能力划分：

无害型——除了传染时减少磁盘的可用空间外，对系统没有其它影响。

无危险型——这类病毒仅仅是减少内存、显示图像、发出声音及同类影响。

危险型——这类病毒在计算机系统操作中造成严重的错误。

非常危险型——这类病毒删除程序、破坏数据、清除系统内存区和操作系统中重要的信息。

根据算法划分：

伴随型病毒——这类病毒并不改变文件本身，它们根据算法产生EXE文件的伴随体，具有同样的名字和不同的扩展名（COM），例如：XCOPY.EXE的伴随体是XCOPY-COM。病毒把自身写入COM文件并不改变EXE文件，当DOS加载文件时，伴随体优先被执行到，再由伴随体加载执行原来的EXE文件。

“蠕虫”型病毒——通过计算机网络传播，不改变文件和资料信息，利用网络从一台机器的内存传播到其它机器的内存，计算机将自身的病毒通过网络发送。有时它们在系统存在，一般除了内存不占用其它资源。

寄生型病毒——除了伴随和“蠕虫”型，其它病毒均可称为寄生型病毒，它们依附在系统的引导扇区或文件中，通过系统的功能进行传播，按其算法不同还可细分为以下几类。

练习型病毒，病毒自身包含错误，不能进行很好的传播，例如一些病毒在调试阶段。

诡秘型病毒，它们一般不直接修改DOS中断和扇区数据，而是通过设备技术和文件缓冲区等对DOS内部进行修改，不易看到资源，使用比较高级的技术。利用DOS空闲的数据区进行工作。

变型病毒（又称幽灵病毒），这一类病毒使用一个复杂的算法，使自己每传播一份都具有不同的内容和长度。它们一般的作法是一段混有无关指令的解码算法和被变化过的病毒体组成。

## 命名

计算机病毒命名，DOS系统下病毒无前缀。*（一般病毒命名格式：<前缀>.<病毒名>.<后缀>） [27]*

|  |  |
| --- | --- |
| **前缀** | **含义** |
| WM | Word6.0、Word95[宏病毒](https://baike.baidu.com/item/%E5%AE%8F%E7%97%85%E6%AF%92" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank) |
| WM97 | Word97宏病毒 |
| XM | [Excel](https://baike.baidu.com/item/Excel" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)5.0、Excel95宏病毒 |
| X97M | Excel5.0和Excel97版本下发作 |
| XF | Excel程序病毒 |
| AM | [Access](https://baike.baidu.com/item/Access" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)95宏病毒 |
| AM97M | Access97宏病毒 |
| W95 | Windows95、98病毒 |
| Win | Windows3.x病毒 |
| W32 | [32位](https://baike.baidu.com/item/32%E4%BD%8D" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)病毒，感染所有32位Windows系统 |
| WINT | 32位Windows病毒，只感染Windows NT |
| Trojan/Troj | [特洛伊木马](https://baike.baidu.com/item/%E7%89%B9%E6%B4%9B%E4%BC%8A%E6%9C%A8%E9%A9%AC" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank) |
| VBS | [VBScript](https://baike.baidu.com/item/VBScript" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)程序语言编写的病毒 |
| VSM | Visio VBA宏或script的宏或script病毒 |
| JS | [JScript](https://baike.baidu.com/item/JScript" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)编程语言编写的病毒 |
| PE | 32位寻址的Windows病毒 |
| OSX | [OS X](https://baike.baidu.com/item/OS X" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)的病毒 |
| OSXL | [OS X Lion](https://baike.baidu.com/item/OS X Lion" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)或者更新版本的病毒 |

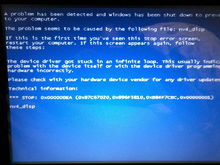
## 征兆预防

### 病毒征兆

屏幕上出现不应有的[特殊](https://baike.baidu.com/item/%E7%89%B9%E6%AE%8A" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)字符或[图像](https://baike.baidu.com/item/%E5%9B%BE%E5%83%8F" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)、[字符](https://baike.baidu.com/item/%E5%AD%97%E7%AC%A6" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)无规则变或[脱落](https://baike.baidu.com/item/%E8%84%B1%E8%90%BD" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)、[静止](https://baike.baidu.com/item/%E9%9D%99%E6%AD%A2/33168" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)、[滚动](https://baike.baidu.com/item/%E6%BB%9A%E5%8A%A8" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)、[雪花](https://baike.baidu.com/item/%E9%9B%AA%E8%8A%B1/79474" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)、[跳动](https://baike.baidu.com/item/%E8%B7%B3%E5%8A%A8" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)、小球亮点、莫名其妙的[信息](https://baike.baidu.com/item/%E4%BF%A1%E6%81%AF" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)提等。

发出[尖叫](https://baike.baidu.com/item/%E5%B0%96%E5%8F%AB" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)、蜂鸣音或非正常[奏乐](https://baike.baidu.com/item/%E5%A5%8F%E4%B9%90" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)等。

经常[无故](https://baike.baidu.com/item/%E6%97%A0%E6%95%85" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)死机，随机地发生重新启动或无法正常[启动](https://baike.baidu.com/item/%E5%90%AF%E5%8A%A8" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)、运行速度明显[下降](https://baike.baidu.com/item/%E4%B8%8B%E9%99%8D" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)、[内存](https://baike.baidu.com/item/%E5%86%85%E5%AD%98" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)空间变小、[磁盘驱动器](https://baike.baidu.com/item/%E7%A3%81%E7%9B%98%E9%A9%B1%E5%8A%A8%E5%99%A8" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)以及其他设备无缘无故地

[](https://baike.baidu.com/pic/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/174112/0/d833c895d143ad4bb1cc0cdb8f025aafa50f06ce?fr=lemma%26ct=single)磁碟机（2007年） [2]

变成[无效](https://baike.baidu.com/item/%E6%97%A0%E6%95%88" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)设备等现象。

磁盘标号被自动[改写](https://baike.baidu.com/item/%E6%94%B9%E5%86%99" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)、出现异常文件、出现固定的[坏扇区](https://baike.baidu.com/item/%E5%9D%8F%E6%89%87%E5%8C%BA" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)、可用磁盘[空间](https://baike.baidu.com/item/%E7%A9%BA%E9%97%B4/55280" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)变小、文件无故变大、[失踪](https://baike.baidu.com/item/%E5%A4%B1%E8%B8%AA/33040" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)或被改乱、[可执行文件](https://baike.baidu.com/item/%E5%8F%AF%E6%89%A7%E8%A1%8C%E6%96%87%E4%BB%B6" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)（*[exe](https://baike.baidu.com/item/exe" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)*）变得无法运行等。

打印异常、打印速度明显[降低](https://baike.baidu.com/item/%E9%99%8D%E4%BD%8E" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)、不能打印、不能打印[汉字](https://baike.baidu.com/item/%E6%B1%89%E5%AD%97" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)与[图形](https://baike.baidu.com/item/%E5%9B%BE%E5%BD%A2" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)等或打印时出现[乱码](https://baike.baidu.com/item/%E4%B9%B1%E7%A0%81" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)。

收到来历不明的[电子邮件](https://baike.baidu.com/item/%E7%94%B5%E5%AD%90%E9%82%AE%E4%BB%B6" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)、自动[链接](https://baike.baidu.com/item/%E9%93%BE%E6%8E%A5" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)到陌生的[网站](https://baike.baidu.com/item/%E7%BD%91%E7%AB%99" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)、[自动](https://baike.baidu.com/item/%E8%87%AA%E5%8A%A8" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)发送电子邮件等。 [28-29] 

### 保护预防

程序或数据[神秘](https://baike.baidu.com/item/%E7%A5%9E%E7%A7%98/4780" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)地消失了，文件名不能[辨认](https://baike.baidu.com/item/%E8%BE%A8%E8%AE%A4" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)等；注意对系统文件、可[执行](https://baike.baidu.com/item/%E6%89%A7%E8%A1%8C/3012" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)文件和数据写[保护](https://baike.baidu.com/item/%E4%BF%9D%E6%8A%A4/33190" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)；不使用来历不明的程序或数据；尽量不用[软盘](https://baike.baidu.com/item/%E8%BD%AF%E7%9B%98" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)进行系统引导。

不轻易打开来历不明的[电子邮件](https://baike.baidu.com/item/%E7%94%B5%E5%AD%90%E9%82%AE%E4%BB%B6" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)；使用新的计算机系统或[软件](https://baike.baidu.com/item/%E8%BD%AF%E4%BB%B6/12053" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)时，先[杀毒](https://baike.baidu.com/item/%E6%9D%80%E6%AF%92" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)后使用；[备份](https://baike.baidu.com/item/%E5%A4%87%E4%BB%BD" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)系统和[参数](https://baike.baidu.com/item/%E5%8F%82%E6%95%B0" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)，建立系统的[应急](https://baike.baidu.com/item/%E5%BA%94%E6%80%A5" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)计划等。[安装](https://baike.baidu.com/item/%E5%AE%89%E8%A3%85" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)杀毒软件。[分类](https://baike.baidu.com/item/%E5%88%86%E7%B1%BB/6000746" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)管理数据。

[29-30]

## 免杀技术以及新特征

免杀是指：对病毒的处理，使之躲过[杀毒软件](https://baike.baidu.com/item/%E6%9D%80%E6%AF%92%E8%BD%AF%E4%BB%B6" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)查杀的一种技术。通常病毒刚从病毒作者手中传播出去前，本身就是免杀的，甚至可以说“病毒比杀毒软件还新，所以杀毒软件根本无法识别它是病毒”，但由于传播后部分用户中毒向杀毒软件公司举报的原因，就会引起安全公司的注意并将之[特征码](https://baike.baidu.com/item/%E7%89%B9%E5%BE%81%E7%A0%81" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)收录到自己的[病毒库](https://baike.baidu.com/item/%E7%97%85%E6%AF%92%E5%BA%93" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)当中，病毒就会被杀毒软件所识别。 [31]

病毒作者可以通过对病毒进行再次保护如使用[汇编](https://baike.baidu.com/item/%E6%B1%87%E7%BC%96" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)加[花指令](https://baike.baidu.com/item/%E8%8A%B1%E6%8C%87%E4%BB%A4" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)或者给文档[加壳](https://baike.baidu.com/item/%E5%8A%A0%E5%A3%B3" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)就可以轻易躲过杀毒软件的病毒特征码库而免于被杀毒软件查杀。

美国的[Norton Antivirus](https://baike.baidu.com/item/Norton Antivirus" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)、[McAfee](https://baike.baidu.com/item/McAfee" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)、[PC-cillin](https://baike.baidu.com/item/PC-cillin" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)，俄罗斯的[Kaspersky Anti-Virus](https://baike.baidu.com/item/Kaspersky Anti-Virus" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)，斯洛伐克的[NOD32](https://baike.baidu.com/item/NOD32" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)等产品在国际上口碑较好，但杀毒、查壳能力都有限，目前病毒库总数量也都仅在数十万个左右。

自我更新性是近年来病毒的又一新特征。病毒可以借助于网络进行变种更新，得到最新的免杀版本的病毒并继续在用户感染的计算机上运行，比如[熊猫烧香](https://baike.baidu.com/item/%E7%86%8A%E7%8C%AB%E7%83%A7%E9%A6%99" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)病毒的作者就创建了“病毒升级[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)”，在最勤时一天要对病毒升级8次，比有些杀毒软件病毒库的更新速度还快，所以就造成了杀毒软件无法识别病毒。

除了自身免杀自我更新之外，很多病毒还具有了对抗它的“天敌”杀毒软件和防火墙产品反病毒软件的全新特征，只要病毒运行后，病毒会自动破坏中毒者计算机上安装的杀毒软件和[防火墙](https://baike.baidu.com/item/%E9%98%B2%E7%81%AB%E5%A2%99/52767" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)产品，如病毒自身驱动级Rootkit保护强制检测并退出杀毒软件进程，可以过主流杀毒软件“主动防御”和穿透软、[硬件](https://baike.baidu.com/item/%E7%A1%AC%E4%BB%B6" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)还原的[机器狗](https://baike.baidu.com/item/%E6%9C%BA%E5%99%A8%E7%8B%97/34383" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)，自动修改系统时间导致一些杀毒软件厂商的正版认证作废以致杀毒软件作废，从而病毒生存能力更加强大。

免杀技术的泛滥使得同一种原型病毒理论上可以派生出近乎无穷无尽的变种，给依赖于特征码技术检测的杀毒软件带来很大困扰。近年来，国际反病毒行业普遍开展了各种前瞻性技术研究，试图扭转过分依赖特征码所产生的不利局面。目前比较有代表性产品的是基于虚拟机技术的启发式扫描软件，代表厂商NOD32，Dr.Web，和基于行为分析技术的主动防御软件，代表厂商中国的[微点主动防御软件](https://baike.baidu.com/item/%E5%BE%AE%E7%82%B9%E4%B8%BB%E5%8A%A8%E9%98%B2%E5%BE%A1%E8%BD%AF%E4%BB%B6" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92/_blank)等。 [32]