病毒的危害

1．病毒激发对计算机数据信息的直接破坏作用 大部分病毒在激发的时候直接破坏计算机的重要信息数据，所利用的手段有格式化磁盘、改写文件分配表和目录 区、删除重要文件或者用无意义的“垃圾”数据改写文件、破坏 CMO5 设置等。 磁盘杀手病毒（D1SK KILLER），内含计数器，在硬盘染毒后累计开机时间 48 小时内激发，激发的时候屏幕上显 示

“Warning!! Don'tturn off power or remove diskette while Disk Killer is Prosessing！”（警 告！D1SK KILLER ll1 在工作，不要关闭电源或取出磁盘），改写硬盘数据。被 D1SK KILLER 破坏的硬盘可以用杀毒 软件修复，不要轻易放弃。

2．占用磁盘空间和对信息的破坏 寄生在磁盘上的病毒总要非法占用一部分磁盘空间。 引导型病毒的一般侵占方式是由病毒本身占据磁盘引导扇区，而把原来的引导区转移到其他扇区，也就是引导型 病毒要覆盖一个磁盘扇区。被覆盖的扇区数据永久性丢失 ,无法恢复。文件型病毒利用一些 DOS 功能进行传染，这些 DOS 功能能够检测出磁盘的未用空间 ,把病毒的传染部分写到磁盘的 未用部位去。所以在传染过程中一般不破坏磁盘上的原有数据，但非法侵占了磁盘空间。一些文件型病毒传染速度很 快，在短时间内感染大量文件，每个文件都不同程度地加长了，就造成磁盘空间的严重浪费。

3．抢占系统资源 除 VIENNA、CASPER 等少数病毒外，其他大多数病毒在动态下都是常驻内存的，这就必然抢占一部分系统资源。病 毒所占用的基本内存长度大致与病毒本身长度相当。病毒抢占内存，导致内存减少，一部分软件

不能运行。除占用内 存外，病毒还抢占中断，干扰系统运行。计算机操作系统的很多功能是通过中断调用技术来实现的。病毒为了传染激 发，总是修改一些有关的中断地址，在正常中断过程中加入病毒的“私货”，从而干扰了系统的正常运行。

4．影响计算机运行速度 病毒进驻内存后不但干扰系统运行，还影响计算机速度，主要表现在：

（1）病毒为了判断传染激发条件，总要对计算机的工作状态进行监视， 这相对于计算机的正常运行状态既多余 又有害。

（2）有些病毒为了保护自己，不但对磁盘上的静态病毒加密，而且进驻内存后的动态病毒也处在加密状态，CPU 每次寻址到病毒处时要运行一段解密程序把加密的病毒解密成合法的 CPU 指令再执行；而病毒运行结束时再用一段程 序对病毒重新加密。这样 CPU 额外执行数千条以至上万条指令。

（3）病毒在进行传染时同样要插入非法的额外操作，特别是传染软盘时不但计算机速度明显变慢， 而且软盘正 常的读写顺序被打乱，发出刺耳的噪声。

5.计算机病毒错误与不可预见的危害 计算机病毒与其他计算机软件的一大差别是病毒的无责任性。编制一个完善的计算机软件需要耗费大量的人力、 物力，经过长时间调试完善，软件才能推出。但在病毒编制者看来既没有必要这样做，也不可能这样做。很多计算机 病毒都是个别人在一台计算机上匆匆编制调试后就向外抛出。反病毒专家在分析大量病毒后发现绝大部分病毒都存在 不同程度的错误。 错误病毒的另一个主要来源是变种病毒。有些初学计算机者尚不具备独立编制软件的能力，出于好奇或其他原因 修改别人的病毒，造成错误。计算机病毒错误所产生的后果往往是不可预见的，反病毒工作者曾经详细指出黑色

星期五病毒存在 9 处错误， 乒 乓病毒有 5 处错误等。但是人们不可能花费大量时间去分析数万种病毒的错误所在。

怎么知道计算机感染了病毒：

1：死机、黑屏、蓝屏或非法操作

2：应用软件不能运行

3：电脑速度明显下降

4：设备被禁用、数据不能保存

5：局域网环境下，能造成网络堵塞，服务器不能正常工作。

计算机病毒的预防措施：

病毒的传染无非是两种方式：一是网络，二是软盘与光盘。如今由于电子邮件的盛行，通过互联网传递的病毒要远远高于后者。

1、不要轻易下载小网站的软件与程序。

2、不要光顾那些很诱惑人的小网站，因为这些网站很有可能就是网络陷阱。

3、不要随便打开某些来路不明的 E-mail 与附件程序。

4、安装正版杀毒软件公司提供的防火墙，并注意时时打开着。

5、不要在线启动、阅读某些文件，否则您很有可能成为网络病毒的传播者。

6、经常给自己发封 E-mail ,看看是否会收到第二封未属标题及附带程序的邮件。