计算机病毒的特点

作者：小六 来源：网友投稿

本文原地址：https://www.xiaorob.com/fanwen/cankao/15397.html

计算机病毒的特点

阅读精选（1）：

计算机病毒的特点有：寄生性、传染性、潜伏性、隐蔽性、破坏性、可触发性等，本文将为您详细介绍计算机病毒的特点以及预防措施。

寄生性

计算机病毒寄生在其他程序之中，当执行这个程序时，病毒就起破坏作用，而在未启动这个程序之前，它是不易被人发觉的。

传染性

计算机病毒不但本身具有破坏性，更有害的是具有传染性，一旦病毒被复制或产生变种，其速度之快令人难以预防。传染性是病毒的基本特征。在生物界，病毒透过传染从一个生物体扩散到另一个生物体。在适当的条件下，它可得到超多繁殖，并使被感染的生物体表现出病症甚至死亡。同样，计算机病毒也会透过各种渠道从已被感染的计算机扩散到未被感染的计算机，在某些状况下造成被感染的计算机工作失常甚至瘫痪。与生物病毒不一样的是，计算机病毒是一段人为编制的计算机程序代码，这段程序代码一旦进入计算机并得以执行，它就会搜寻其他贴合其传染条件的程序或存储介质，确定目标后再将自身代码插入其中，到达自我繁殖的目的。只要一台计算机染毒，如不及时处理，那么病毒会在这台机子上迅速扩散，计算机病毒可透过各种可能的渠道，如软盘、计算机网络去传染其他的计算机。当您在一台机器上发现了病毒时，往往曾在这台计算机上用过的软盘已感染上了病毒，而与这台机器相联网的其他计算机也许也被该病毒染上了。是否具有传染性是判别一个程序是否为计算机病毒的最重要条件。病毒程序透过修改磁盘扇区信息或文件资料并把自身嵌入到其中的方法到达病毒的传染和扩散。被嵌入的程序叫做宿主程序；

潜伏性

有些病毒像定时炸弹一样，让它什么时间发作是预先设计好的。比如黑色星期五病毒，不到预定时间一点都觉察不出来，等到条件具备的时候一下子就爆炸开来，对系统进行破坏。一个编制精巧的计算机病毒程序，进入系统之后一般不会立刻发作，因此病毒能够静静地躲在磁盘或磁带里呆上几天，甚至几年，一旦时机成熟，得到运行机会，就又要四处繁殖、扩散，继续为害。潜伏性的第二种表现是指，计算机病毒的内部往往有一种触发机制，不满足触发条件时，计算机病毒

除了传染外不做什么破坏。触发条件一旦得到满足，有的在屏幕上显示信息、图形或特殊标识，有的则执行破坏系统的操作，如格式化磁盘、删除磁盘文件、对数据文件做加密、封锁键盘以及使系统死锁等；

隐蔽性

计算机病毒具有很强的隐蔽性，有的能够透过病毒软件检查出来，有的根本就查不出来，有的时隐时现、变化无常，这类病毒处理起来通常很困难。

破坏性

计算机中毒后，可能会导致正常的程序无法运行，把计算机内的文件删除或受到不一样程度的损坏。通常表现为：增、删、改、移。

可触发性

病毒因某个事件或数值的出现，诱使病毒实施感染或进行攻击的特性称为可触发性。为了隐蔽自我，病毒务必潜伏，少做动作。如果完全不动，一向潜伏的话，病毒既不能感染也不能进行破坏，便失去了杀伤力。病毒既要隐蔽又要维持杀伤力，它务必具有可触发性。病毒的触发机制就是用来控制感染和破坏动作的频率的。病毒具有预定的触发条件，这些条件可能是时间、日期、文件类型或某些特定数据等。病毒运行时，触发机制检查预定条件是否满足，如果满足，启动感染或破坏动作，使病毒进行感染或攻击；如果不满足，使病毒继续潜伏。

阅读精选（2）：

计算机病毒一般具有以下特性：

1. 计算机病毒的程序性（可执行性）

计算机病毒与其他合法程序一样，是一段可执行程序，但它不是一个完整的程序，而是寄生在其他可执行程序上，

因此它享有一切程序所能得到的权力。在病毒运行时，与合法程序争夺系统的控制权。计算机病毒只有当它在计算机

内得以运行时，才具有传染性和破坏性等活性。也就是说计算机CPU的控制权是关键问题。若计算机在正常程序控制

下运行，而不运行带病毒的程序，则这台计算机总是可靠的。在这台计算机上能够查看病毒文件的名字，查看计算机

病毒的代码，打印病毒的代码，甚至拷贝病毒程序，却都不会感染上病毒。反病毒技术人员整天就是在这样的环境下

工作。他们的计算机虽也存有各种计算机病毒的代码，但已置这些病毒于控制之下，计算机不会运行病毒程序，整个

系统是安全的。相反，计算机病毒一经在计算机上运行，在同一台计算机内病毒程序与正常系统程序，或某种病毒与

其他病毒程序争夺系统控制权时往往会造成系统崩溃，导致计算机瘫痪。反病毒技术就是要提前取得计算机系统的控

制权，识别出计算机病毒的代码和行为，阻止其取得系统控制权。反病毒技术的优劣就是体此刻这一点上。一个好的

抗病毒系统就应不仅仅能可靠地识别出已知计算机病毒的代码，阻止其运行或旁路掉其对系统的控制权（实现安全带毒

运行被感染程序），还就应识别出未知计算机病毒在系统内的行为，阻止其传染和破坏系统的行动。

2. 计算机病毒的传染性

传染性是病毒的基本特征。在生物界，病毒透过传染从一个生物体扩散到另一个生物体。在适当的条件下，它可

得到超多繁殖，并使被感染的生物体表现出病症甚至死亡。同样，计算机病毒也会透过各种渠道从已被感染的计算机

扩散到未被感染的计算机，在某些状况下造成被感染的计算机工作失常甚至瘫痪。与生物病毒不一样的是，计算机病毒

是一段人为编制的计算机程序代码，这段程序代码一旦进入计算机并得以执行，它就会搜寻其他贴合其传染条件的程

序或存储介质，确定目标后再将自身代码插入其中，到达自我繁殖的目的。只要一台计算机染毒，如不及时处理，那

么病毒会在这台机子上迅速扩散，其中的超多文件（一般是可执行文件）会被感染。而被感染的文件又成了新的传染

源，再与其他机器进行数据交换或透过网络接触，病毒会继续进行传染。

正常的计算机程序一般是不会将自身的代码强行连接到其他程序之上的。而病毒却能使自身的代码强行传染到一

切贴合其传染条件的未受到传染的程序之上。计算机病毒可透过各种可能的渠道，如软盘、计算机网络去传染其他的

计算机。当您在一台机器上发现了病毒时，往往曾在这台计算机上用过的软盘已感染上了病毒，而与这台机器相联网

的其他计算机也许也被该病毒染上了。是否具有传染性是判别一个程序是否为计算机病毒的最重要条件。

病毒程序透过修改磁盘扇区信息或文件资料并把自身嵌入到其中的方法到达病毒的传染和扩散。被嵌入的程序叫

做宿主程序。

3．计算机病毒的潜伏性

一个编制精巧的计算机病毒程序，进入系统之后一般不会立刻发作，能够在几周或者几个月内甚至几年内隐藏在

合法文件中，对其他系统进行传染，而不被人发现，潜伏性愈好，其在系统中的存在时间就会愈长，病毒的传染范围

就会愈大。

潜伏性的第一种表现是指，病毒程序不用专用检测程序是检查不出来的，因此病毒能够静静地躲在磁盘或磁带里

呆上几天，甚至几年，一旦时机成熟，得到运行机会，就又要四处繁殖、扩散，继续为害。潜伏性的第二种表现是指，

计算机病毒的内部往往有一种触发机制，不满足触发条件时，计算机病毒除了传染外不做什么破坏。触发条件一旦得

到满足，有的`在屏幕上显示信息、图形或特殊标识，有的则执行破坏系统的操作，如格式化磁盘、删除磁盘文件、对

数据文件做加密、封锁键盘以及使系统死锁等。

4．计算机病毒的可触发性

病毒因某个事件或数值的出现，诱使病毒实施感染或进行攻击的特性称为可触发性。为了隐蔽自我，病毒务必潜

伏，少做动作。如果完全不动，一向潜伏的话，病毒既不能感染也不能进行破坏，便失去了杀伤力。病毒既要隐蔽又

要维持杀伤力，它务必具有可触发性。病毒的触发机制就是用来控制感染和破坏动作的频率的。病毒具有预定的触发

条件，这些条件可能是时间、日期、文件类型或某些特定数据等。病毒运行时，触发机制检查预定条件是否满足，如

果满足，启动感染或破坏动作，使病毒进行感染或攻击；如果不满足，使病毒继续潜伏。

5．计算机病毒的破坏性

所有的计算机病毒都是一种可执行程序，而这一可执行程序又必然要运行，所以对系统来讲，所有的计算机病毒

都存在一个共同的危害，即降低计算机系统的工作效率，占用系统资源，其具体状况取决于入侵系统的病毒程序。

同时计算机病毒的破坏性主要取决于计算机病毒设计者的目的，如果病毒设计者的目的在于彻底破坏系统的正常

运行的话，那么这种病毒对于计算机系统进行攻击造成的后果是难以设想的，它能够毁掉系统的部分数据，也能够破

坏全部数据并使之无法恢复。

但并非所有的病毒都对系统产生极其恶劣的破坏作用。有时几种本没有多大破坏作用的病毒交叉感染，也会导致系统

崩溃等重大恶果。

6．攻击的主动性

病毒对系统的攻击是主动的，不以人的意志为转移的。也就是说，从必须的程度上讲，计算机系统无论采取多

么严密的保护措施都不可能彻底地排除病毒对系统的攻击，而保护措施充其量是一种预防的手段而已。

7．病毒的针对性

计算机病毒是针对特定的计算机和特定的操作系统的。例如，有针对1BMPC机及其兼容机的，有针对Apple公司

的Macintosh的，还有针对UNIX操作系统的。例如小球病毒是针对IBMPC机及其兼容机上的DOS操作系统的。

8．病毒的非授权性

病毒未经授权而执行。一般正常的程序是由用户调用，再由系统分配资源，完成用户交给的任务。其目的对用户

是可见的、透明的。而病毒具有正常程序的一切特性，它隐藏在正常程序中，当用户调用正常程序时窃取到系统的控

制权，先于正常程序执行，病毒的动作、目的对用户是未知的，是未经用户允许的。

9．病毒的隐蔽性

病毒一般是具有很高编程技巧，短小精悍的程序。通常附在正常程序中或磁盘较隐蔽的地方，也有个别的以隐含

文件形式出现。目的是不让用户发现它的存在。如果不经过代码分析，病毒程序与正常程序是不容易区别开来的。一

般在没有防护措施的状况下，计算机病毒程序取得系统控制权后，能够在很短的时间里传染超多程序。而且受到传染

后，计算机系统通常仍能正常运行，使用户不会感到任何异常，好像不曾在计算机内发生过什么。试想，如果病毒在

传染到计算机上之后，机器立刻无法正常运行，那么它本身便无法继续进行传染了。正是由于隐蔽性，计算机病毒得

以在用户没有察觉的状况下扩散并游荡于世界上百万台计算机中。

大部分的病毒的代码之所以设计得十分短小，也是为了隐藏。病毒一般只有几百或1K字节，而PC机对DOS文件的

存取速度可达每秒几百KB以上，所以病毒转瞬之间便可将这短短的几百字节附着到正常程序之中，使人十分不易察觉。

计算机病毒的隐蔽性表此刻两个方面：

一是传染的隐蔽性，大多数病毒在进行传染时速度是极快的，一般不具有外部表现，不易被人发现。让我们设想，

如果计算机病毒每当感染一个新的程序时都在屏幕上显示一条信息“我是病毒程序，我要干坏事了”，那么计算机病

毒早就被控制住了。确实有些病毒十分“勇于暴露自我”，时不时在屏幕上显示一些图案或信息，或演奏一段乐曲。

往往此时那台计算机内已有许多病毒的拷贝了。许多计算机用户对计算机病毒没有任何概念，更不用说心理上的警惕

了。他们见到这些新奇的屏幕显示和音响效果，还以为是来自计算机系统，而没有意识到这些病毒正在损害计算机系

统，正在制造灾难。

二是病毒程序存在的隐蔽性，一般的病毒程序都夹在正常程序之中，很难被发现，而一旦病毒发作出来，往往已

经给计算机系统造成了不一样程度的破坏。被病毒感染的计算机在多数状况下仍能维持其部分功能，不会由于一感染上

病毒，整台计算机就不能启动了，或者某个程序一旦被病毒所感染，就被损坏得不能运行了，如果出现这种状况，病

毒也就不能流传于世了。计算机病毒设计的精巧之处也在那里。正常程序被计算机病毒感染后，其原有功能基本上不

受影响，病毒代码附于其上而得以存活，得以不断地得到运行的机会，去传染出更多的复制体，与正常程序争夺系统

的控制权和磁盘空间，不断地破坏系统，导致整个系统的瘫痪。病毒的代码设计得十分精巧而又短小。

10．病毒的衍生性

这种特性为一些好事者带给了一种创造新病毒的捷径。

分析计算机病毒的结构可知，传染的破坏部分反映了设计者的设计思想和设计目的。但是，这能够被其他掌握原

理的人以其个人的企图进行任意改动，从而又衍生出一种不一样于原版本的新的计算机病毒（又称为变种）。这就是计

算机病毒的衍生性。这种变种病毒造成的后果可能比原版病毒严重得多。

11．病毒的寄生性（依附性）

病毒程序嵌入到宿主程序中，依靠于宿主程序的执行而生存，这就是计算机病毒的寄生性。病毒程序在侵入到宿

主程序中后，一般对宿主程序进行必须的修改，宿主程序一旦执行，病毒程序就被激活，从而能够进行自我复制和繁

衍。

12．病毒的不可预见性

从对病毒的检测方面来看，病毒还有不可预见性。不一样种类的病毒，它们的代码千差万别，但有些操作是共有的

（如驻内存，改中断）。有些人利用病毒的这种共性，制作了声称可查所有病毒的程序。这种程

序的确可查出一些新

病毒，但由于目前的软件种类极其丰富，且某些正常程序也使用了类似病毒的操作甚至借鉴了某些病毒的技术。使用

这种方法对病毒进行检测势必会造成较多的误报状况。而且病毒的制作技术也在不断的提高，病毒对反病毒软件永远

是超前的。新一代计算机病毒甚至连一些基本的特征都隐藏了，有时可透过观察文件长度的变化来判别。然而，更新

的病毒也能够在这个问题上蒙蔽用户，它们利用文件中的空隙来存放自身代码，使文件长度不变。许多新病毒则采用

变形来逃避检查，这也成为新一代计算机病毒的基本特征。

13. 计算机病毒的欺骗性

计算机病毒行动诡秘，计算机对其反应迟钝，往往把病毒造成的错误当成事实理解下来，故它很容易获得成功。

14. 计算机病毒的持久性

即使在病毒程序被发现以后，数据和程序以至操作系统的恢复都十分困难。个性是在网络操作状况下，由于病毒

程序由一个受感染的拷贝透过网络系统反复传播，使得病毒程序的清除十分复杂。

阅读精选（3）：

计算机病毒的特征

(一)非授权可执行性用户通常调用执行一个程序时，把系统控制交给这个程序，并分配给他相应系统资源，如内存，从而使之能够运行完成用户的需求。因此程序执行的过程对用户是透明的。而计算机病毒是非法程序，正常用户是不会明知是病毒程序，而故意调用执行。但由于计算机病毒具有正常程序的一切特性:可存储性、可执行性。它隐藏在合法的程序或数据中，当用户运行正常程序时，病毒伺机窃取到系统的控制权，得以抢先运行，然而此时用户还认为在执行正常程序。

(二)隐蔽性计算机病毒是一种具有很高编程技巧、短小精悍的可执行程序。它通常粘附在正常程序之中或磁盘引导扇区中，或者磁盘上标为坏簇的扇区中，以及一些空闲概率较大的扇区中，这是它的非法可存储性。病毒想方设法隐藏自身，就是为了防止用户察觉。

(三)传染性传染性是计算机病毒最重要的特征，是决定一段程序代码是否为计算机病毒的依据。病毒程序一旦侵入计算机系统就开始搜索能够传染的程序或者磁介质，然后透过自我复制迅速传播。由于目前计算机网络日益发达，计算机病毒能够在极短的时间内，透过像Internet这样的网

络传遍世界。

(四)潜伏性计算机病毒具有依附于其他媒体而寄生的潜力，这种媒体我们称之为计算机病毒的宿主。依靠病毒的寄生潜力，病毒传染合法的程序和系统后，不立即发作，而是悄悄隐藏起来，然后在用户不察觉的状况下进行传染。这样，病毒的潜伏性越好，它在系统中存在的时间也就越长，病毒传染的范围也越广，其危害性也越大。

(五)表现性或破坏性无论何种病毒程序一旦侵入系统都会对操作系统的运行造成不一样程度的影响。即使不直接产生破坏作用的病毒程序也要占用系统资源(如占用内存空间，占用磁盘存储空间以及系统运行时间等)。而绝大多数病毒程序要显示一些文字或图像，影响系统的正常运行，还有一些病毒程序删除文件，加密磁盘中的数据，甚至摧毁整个系统和数据，使之无法恢复，造成无可挽回的损失。因此，病毒程序的副作用轻者降低系统工作效率，重者导致系统崩溃、数据丢失。病毒程序的表现性或破坏性体现了病毒设计者的真正意图。

(六)可触发性计算机病毒一般都有一个或者几个触发条件。满足其触发条件或者激活病毒的传染机制，使之进行传染;或者激活病毒的表现部分或破坏部分。触发的实质是一种条件的控制，病毒程序能够依据设计者的要求，在必须条件下实施攻击。这个条件能够是敲入特定字符，使用特定文件，某个特定日期或特定时刻，或者是病毒内置的计数器到达必须次数等。