病毒分类

按破坏性分

(1) 良性病毒 (2) 恶性病毒 (3) 极恶性病毒 (4) 灾难性病毒　按传染方式分

(1) 引导区型病毒

引导区型病毒主要通过软盘在操作系统中传播，感染引导区，蔓延到硬盘，并能感染到硬盘中的"主引导记录"。

(2) 文件型病毒

文件型病毒是文件感染者，也称为寄生病毒。它运行在计算机存储器中，通常感染扩展名为 COM、EXE、SYS 等类型的文件。

(3) 混合型病毒

混合型病毒具有引导区型病毒和文件型病毒两者的特点。

(4) 宏病毒

宏病毒是指用 BASIC 语言编写的病毒程序寄存在 Office 文档上的宏代码。宏病毒影响对文档的各种操作。

按连接方式分

(1) 源码型病毒

它攻击高级语言编写的源程序，在源程序编译之前插入其中，并随源程序一起编译、连接成可执行文件。源码型病毒较为少见，亦难以编写。

(2) 入侵型病毒

入侵型病毒可用自身代替正常程序中的部分模块或堆栈区。因此这类病毒只攻击某些特定程序，针对性强。一般情况下也难以被发现，清除起来也较困难。

(3) 操作系统型病毒

操作系统型病毒可用其自身部分加入或替代操作系统的部分功能。因其直接感染操作系统，这类病毒的危害性也较大。

⑷ 外壳型病毒

外壳型病毒通常将自身附在正常程序的开头或结尾，相当于给正常程序加了个外壳。大部份的文件型病毒都属于这一类。

下面附带一些常见的病毒前缀的解释（针对我们用得最多的 Windows*作系统）：

1、系统病毒

系统病毒的前缀为：Win32、PE、Win95、W32、W95 等。这些病毒的一般公有的特性是可以感染 windows*作系统的 *.exe 和 *.dll 文件，并通过这些文件进行传播。如 CIH 病毒。

2、蠕虫病毒

蠕虫病毒的前缀是：Worm。这种病毒的公有特性是通过网络或者系统漏洞进行传播，很大部分的蠕虫病毒都有向外发送带毒邮件，阻塞网络的特性。比如冲击波（阻塞网络），小邮差（发带毒邮件）等。

3、木马病毒、黑客病毒

木马病毒其前缀是：Trojan，黑客病毒前缀名一般为 Hack 。木马病毒的公有特性是通过网络或者系统漏洞进入用户的系统并隐藏，然后向外界泄露用户的信息，而黑客病毒则有一个可视的界面，能对用户的电脑进行远程控制。木马、黑客病毒往往是成对出现的，即木马病毒负责侵入用户的电脑，而黑客病毒则会通过该木马病毒来进行控制。现在这两种类型都越来越趋向于整合了。一般的木马如 QQ 消息尾巴木马 Trojan.QQ3344 ，还有大家可能遇见比较多的针对网络

游戏的木马病毒如 Trojan.LMir.PSW.60 。这里补充一点，病毒名中有 PSW 或者什么 PWD 之类的一般都表示这个病毒有盗取密码的功能(这些字母一般都为“密码”的英文“password”的缩写）一些黑客程序如：网络枭雄（Hack.Nether.Client）等。

4、脚本病毒

脚本病毒的前缀是：Script。脚本病毒的公有特性是使用脚本语言编写，通过网页进行的传播的病毒，如红色代码（Script.Redlof）。脚本病毒还会有如下前缀：VBS、JS（表明是何种脚本编写的），如欢乐时光（VBS.Happytime）、十四日（Js.Fortnight.c.s）等。

5、宏病毒

其实宏病毒是也是脚本病毒的一种，由于它的特殊性，因此在这里单独算成一类。宏病毒的前缀是：Macro，第二前缀是：Word、Word97、Excel、Excel97（也许还有别的）其中之一。凡是只感染 WORD97 及以前版本 WORD 文档的病毒采用 Word97 做为第二前缀，格式是：Macro.Word97；凡是只感染 WORD97 以后版本 WORD 文档的病毒采用 Word 做为第二前缀，格式是：Macro.Word ;凡是只感染 EXCEL97 及以前版本 EXCEL 文档的病毒采用 Excel97 做为第二前缀 ,格式是 :Macro.Excel97 ;凡是只感染 EXCEL97 以后版本 EXCEL 文档的病毒采用 Excel 做为第二前缀，格式是：Macro.Excel，依此类推。该类病毒的公有特性是能感染 OFFICE 系列文档，然后通过 OFFICE 通用模板进行传播，如：著名的美丽莎(Macro.Melissa)。

6、后门病毒

后门病毒的前缀是：Backdoor。该类病毒的公有特性是通过网络传播，给系统

开后门，给用户电脑带来安全隐患。如很多朋友遇到过的 IRC 后门 Backdoor.IRCBot 。

7、病毒种植程序病毒

这类病毒的公有特性是运行时会从体内释放出一个或几个新的病毒到系统目录下，由释放出来的新病毒产生破坏。如：冰河播种者（Dropper.BingHe2.2C）、MSN 射手(Dropper.Worm.Smibag)等。

8．破坏性程序病毒

破坏性程序病毒的前缀是：Harm。这类病毒的公有特性是本身具有好看的图标来诱惑用户点击，当用户点击这类病毒时，病毒便会直接对用户计算机产生破坏。如：格式化 C 盘（Harm.formatC.f）、杀手命令（Harm.Command.Killer）等。

9．玩笑病毒

玩笑病毒的前缀是：Joke。也称恶作剧病毒。这类病毒的公有特性是本身具有好看的图标来诱惑用户点击，当用户点击这类病毒时，病毒会做出各种破坏*作来吓唬用户，其实病毒并没有对用户电脑进行任何破坏。如：女鬼（Joke.Girlghost）病毒。

10．捆绑机病毒

捆绑机病毒的前缀是：Binder。这类病毒的公有特性是病毒作者会使用特定的捆绑程序将病毒与一些应用程序如 QQ、IE 捆绑起来，表面上看是一个正常的文件，当用户运行这些捆绑病毒时，会表面上运行这些应用程序，然后隐藏运行捆绑在一起的病毒，从而给用户造成危害。如：捆绑 QQ（Binder.QQPass.QQBin）、系统杀手（Binder.killsys）等。

以上为比较常见的病毒前缀，有时候我们还会看到一些其他的，但比较少见，这里简单提一下：

DoS：会针对某台主机或者服务器进行 DoS 攻击； Exploit：会自动通过溢出对方或者自己的系统漏洞来传播自身，或者他本身就是一个用于 Hacking 的溢出工具；

HackTool：黑客工具，也许本身并不破坏你的机子，但是会被别人加以利用来用你做替身去破坏别人。

你可以在查出某个病毒以后通过以上所说的方法来初步判断所中病毒的基本情况，达到知己知彼的效果。在杀毒无法自动查杀，打算采用手工方式的时候这些信息会给你很大的帮助。