蠕虫病毒

蠕虫病毒是一种常见的计算机病毒。它是利用网络进行复制和传播，传染途径是通过网络和电子邮件。最初的蠕虫病毒定义是因为在 DOS 环境下，病毒发作时会在屏幕上出现一条类似虫子的东西，胡乱吞吃屏幕上的字母并将其改形。蠕虫病毒是自包含的程序（或是一套程序），它能传播自身功能的拷贝或自身的某些部分到其他的计算机系统中（通常是经过网络连接）。

蠕虫病毒是自包含的程序(或是一套程序),它能传播它自身功能的拷贝或它的某些部分到其他的计算机系统中(通常是经过网络连接)。请注意，与一般病毒不同，蠕虫不需要将其自身附着到宿主程序，有两种类型的蠕虫：主机蠕虫与网络蠕虫。主计算机蠕虫完全包含在它们运行的计算机中，并且使用网络的连接仅将自身拷贝到其他的计算机中，主计算机蠕虫在将其自身的拷贝加入到另外的主机后，就会终止它自身(因此在任意给定的时刻，只有一个蠕虫的拷贝运行)，这种蠕虫有时也叫"野兔"，蠕虫病毒一般是通过 1434 端口漏洞传播。

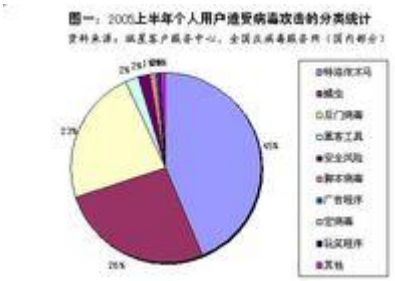
比如近几年危害很大的“尼姆亚”病毒就是蠕虫病毒的一种，2007 年 1 月流行的“熊猫烧香”以及其变种也是蠕虫病毒。这一病毒利用了微软视窗操作系统的漏洞，计算机感染这一病毒后，会不断自动拨号上网，并利用文件中的地址信息或者网络共享进行传播，最终破坏用户的大部分重要数据。

在 QQ 群下载的分享文件打开后会跳转到色情网站。这是流行的 QQ 群蠕虫病毒，不仅会感染 PC，安卓手机甚至未越狱的 iPhone 和 iPad 也无法幸免。

形成原因

漏洞攻击

利用操作系统和应用程序的漏洞主动进行攻击



蠕虫病毒

此类病毒主要是“红色代码”和“尼姆亚”，以及依然肆虐的“求职信”等。由于 IE 浏览器的漏洞（IFRAMEEXECCOMMAND），使得感染了“尼姆亚”病毒的邮件在不去手工打开附件的情况下病毒就能激活，而此前即便是很多防病毒专家也一直认为，带有病毒附件的邮件，只要不去打开附件，病毒不会有危害。“红色代码”是利用了微软 IIS 服务器软件的漏洞(idq.dll 远程缓存区溢出)来传播，SQL 蠕虫王病毒则是利用了微软的数据库系统的一个漏洞进行大肆攻击。

方式多样

如“尼姆亚”病毒和”求职信”病毒，可利用的传播途径包括文件、电子邮件、Web 服务器、网络共享等等。

新技术

与传统的病毒不同的是，许多新病毒是利用当前最新的编程语言与编程技术实现的，易于修改以产生新的变种，从而逃避反病毒软件的搜索。另外，新病毒利用 Java、ActiveX、VBScript 等技术，可以潜伏在 HTML 页面里，在上网浏览时触发。

黑客技术

与黑客技术相结合，潜在的威胁和损失更大

以红色代码为例，感染后的机器的 web 目录的\scripts 下将生成一个 root.exe，可以远程执行任何命令，从而使黑客能够再次进入。蠕虫和普通病毒不同的一个特征是蠕虫病毒往往能够利用漏洞，这里的漏洞或者说是缺陷，可以分为两种，即软件上的缺陷和人为的缺陷。软件上的缺陷，如远程溢出、微软 IE 和 Outlook 的自动执行漏洞等等，需要软件厂商和用户共同配合，不断地升级软件。而人为

蠕虫病毒

的缺陷，主要指的是计算机用户的疏忽。这就是所谓的社会工程学（socialengineering），当收到一封邮件带着病毒的求职信邮件时候，大多数人都会抱着好奇去点击的。对于企业用户来说，威胁主要集中在服务器和大型应用软件的安全上，而对个人用户而言，主要是防范第二种缺陷。

在以上分析的蠕虫病毒中，只对安装了特定的微软组件的系统进行攻击，而对广大个人用户而言，是不会安装 IIS（微软的因特网服务器程序，可以允许在网上提供 web 服务）或者是庞大的数据库系统的。因此，上述病毒并不会直接攻击个人用户的电脑（当然能够间接的通过网络产生影响）。但接下来分析的蠕虫病毒，则是对个人用户威胁最大，同时也是最难以根除，造成的损失也更大的

一类蠕虫病毒。对于个人用户而言，威胁大的蠕虫病毒采取的传播方式，一般为电子邮件（Email）以及恶意网页等等。 对于利用电子邮件传播的蠕虫病毒来说，通常利用的是各种各样的欺骗手段诱惑用户点击的方式进行传播。恶意网页确切地讲是一段黑客破坏代码程序，它内嵌在网页中，当用户在不知情的情况下打开含有病毒的网页时，病毒就会发作。这种病毒代码镶嵌技术的原理并不复杂，所以会被很多怀不良企图者利用，在很多黑客网站竟然出现了关于用网页进行破坏的技术的论坛，并提供破坏程序代码下载，从而造成了恶意网页的大面积泛滥，也使越来越多的用户遭受损失。对于恶意网页，常常采取 vbscript 和 javascript 编程的形式，由于编程方式十分的简单，所以在网上非常的流行。

Vbscript 是由微软操作系统的 wsh（WindowsScriptingHostWindows 脚本主机）解析并执行的，由于其编程非常简单，所以此类脚本病毒在网上疯狂传播，疯狂一时的爱虫病毒就是一种 vbs 脚本病毒，然后伪装成邮件附件诱惑用户点击运行。更为可怕的是，这样的病毒是以源代码的形式出现的，只要懂得一点关于脚本编程的人就可以修改其代码，形成各种各样的变种