网络蠕虫

介绍

网络蠕虫是一种智能化、自动化，综合网络攻击、密码学和计算机病毒技术，无须计算机使用者干预即可运行的攻击程序或代码，它会扫描和攻击网络上存在系统漏洞的节点主机，通过局域网或者国际互联网从一个节点传播到另外一个节点”。此定义体现了新一代网络蠕虫智能化、自动 ies 化和高技术化的特征。

定义

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),它能传播它自身功能的拷贝或它（蠕虫病毒）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，它是一种独立智能程序。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（侵占）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 年春天流行“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。

蠕虫病毒的一般防治方法是：使用具有实时监控功能的杀毒软件，并且注意不要轻易打开不熟悉的邮件附件。

计算机蠕虫是怎么发作的

用操作系统和应用程序的漏洞进行攻击

此类病毒主要是“红色代码”和“尼姆亚”，以及至今依然肆虐的”求职信”等。由于 IE 浏览器的漏洞（IFRAME EXECCOMMAND），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。

传播方式多样

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。

病毒制作技术新

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、VB Script 等技术，可以潜伏在 HTML 页面里，在上网浏览时触发。

与黑客技术相结合

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（social engineering），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。