浅析计算机病毒类型及其防护措施

鄢 翔

（河南省开封市技师学院，河南 开封 475004）

摘 要：首先简要的介绍了计算机病毒的分类及自身规律，并对现在最流行的计算机病毒注入进行了深入分析，概括出了计算机病毒的几个明显特征，引申出计算机系统基本的防护知识，从而得出计算机病毒的主要防护方法。

关键词：计算机病毒；防护；类型

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利。自 20 世纪 80 年代莫里斯编制的第一个“蠕虫”病毒程序至今，世界上出现了许多不同类型的病毒，给数以千计的计算机用户造成不可估量的损失。

1 计算机病毒的类型

计算机病毒的类型繁多，在近几年内，主要有以下几种病毒：

1.1 引导性病毒。通过感染磁盘上的引导区或改写磁盘分区表来感染系统，它是一中开机即可启动的病毒，先于操作系统而存在，所以用软盘引导启动的电子计算机容易感染这种病毒。该病毒几乎常驻内存，激活时即可发作。

1.2 文件型病毒。这种病毒将其自身附着在程序文件中，通常感染属性为 COM 和 EXE 的程序文件，但是这类病毒中的一些病毒能够感染任何运行或解释所需要的程序文件。CIH 就是一种典型的文件型病毒。

1.3 蠕虫病毒。计算机蠕虫也可以说是计算机病毒的一种，与病毒不同的是，蠕虫不会感染其他档案。蠕虫的主要特征是会自我复制并主动散播到网络系统上的其他计算机里面。就像虫一样在网络的系统里面爬窜，所以称“蠕虫”。

1.4 特洛伊木马。特洛伊木马是一种计算机程序，伪装成某种有用的或有趣的程序，比如屏幕保护程序、算命程序、计算机游戏等、它可以破坏数据、骗取使用者的密码等等。在学术定义上，特洛伊木马不会自我复制，也不会主动散播到别的计算机里面。

1.5“美丽杀手”(Melissa)病毒。这种病毒是专门针对微软电子邮件服务器 MS Exchange 和电子邮件收发软件 Out1ookExpress 的 Word 宏病毒，是一种拒绝服务的攻击型病毒，能够影响计算机运行微软 Word97、Word2000 和 Outlook。这种病毒是一种 Word 文档附件，由 E-mail 携带传播扩散，能够自我复制，一旦用户打开这个附件，就会使用 Outlook 按收件人的 Outlook 地址簿向前 50 名收件人自动复制发送，从而过载 E-mail 服务器或使之损坏。

1.6“猫癣”病毒。“猫癣”病毒最明显的中毒症状，是电脑桌面上出现 USP10.DLL 文件、迅雷无法启动及安全软件自动关闭，并且伴随网游账号被盗，目标囊括魔兽世界、大话西游 online2、剑侠世界、封神榜 2 等主流游戏，对用户的虚拟财产影响巨大。无论是哪款变种的“猫癣”，都能利用 IE7 Oday 漏洞、微软 access 漏洞、新浪 UC 漏洞、Realplayer 漏洞等多种系统和第三方软件的安全漏洞进行网页挂马传播，如果用户系统存在以上漏洞，又刚好浏览到被挂马的网页，“猫癣”就会乘虚而入。

1.7 机器狗病毒。机器狗病毒因最初的版本采用电子狗的照片做图标而被网民命名为“机器狗”，该病毒变种繁多，多表现为杀毒软件无法正常运行。该病毒的主要危害是充当病毒木马下载器，与 AV 终结者病毒相似，病毒通过修改注册表，让大多数流行的安全软件失效，然后疯狂下载各种盗号工具或黑客工具，给用户电脑带来严重的威胁。机器狗病毒直接操作磁盘以绕过系统文件完整性的检验，通过感染系统文件（比如 explorer.exe，userinit.exe，winhlp32.exe 等）达到隐蔽启动；通过底层技术穿透冰点，影子等还原系统软件导致大量网吧用户感染病毒，无法通过还原来保证系统的安全；通过修复 SSDT（就是恢复安全软件对系统关键 API 的 HOOK），映像挟持，进程操作等方法使得大量的安全软件失去作用；联网下载大量的盗号木马给广大网民的网络虚拟财产造成巨大威胁，部分机器狗变种还会下载 ARP 恶意攻击程序对所在局域网（或者服务器）进行 ARP 欺骗影响网络安全。

2 计算机病毒的特点

2.1 计算机病毒的传染性。传染性是病毒的基本特征，一旦病毒被复制或产生变种，其传染速度之快令人难以预防。计算机病毒会通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。

2.2 计算机病毒的潜伏性。大部分病毒感染系统之后一般不会马上发作，它隐藏在系统之中，就像定时炸弹一样，只有在满足其特定条件时才启动。比如黑色星期五病毒，不到定的时间不会觉察出异常，一旦逢到 13 日的星期五就会爆炸开来，对系统进行破坏。

2.3 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。

2.4 计算机病毒攻击的主动性。病毒对系统的攻击是主动的，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的攻击，而保护措施只能是一种预防手段。

2.5 计算机病毒的隐蔽性。计算机病毒具有很强的隐蔽性，它通常附在正常的程序之中或藏在磁盘的隐蔽地方，有些病毒采用了极其高明的手段来隐藏自己，如使用透明图标、注册表内的相似字符等，而且有的病毒在感染了系统之后，计算机系统仍能正常工作，用户不会感到有任何异常，在这种情况下，普通用户是无法正常的情况下发现病毒的。

3 计算机病毒的防护措施。

3.1 改变计算机的启动次序，将软盘或光盘启动改为计算机硬盘启动，从而减少病毒侵入的路径。

3.2 安装市面上认可度高，功能较为全面的杀毒软件，并每天升级病毒库。随着计算机病毒编制技术和黑客技术的逐步融合，下载、安装安全补丁程序和升级杀毒软件已成为防治计算机病毒的最有效手段。

3.3 经常（每个月）都要定时杀毒一次。

3.4 如果发现病毒，尽量在 DOS 环境，或安全模式下杀毒，从而避免病毒复活的可能。

3.5 从网上下载的文件，或者从另外计算机上拷贝过来的软件，一定要先查毒，确定安全无毒再打开，做到小心谨慎。

3.6 在上网或平时使用时，应打开病毒防火墙。实时保护，可以免受计算机收到病毒的侵害。

3.7 不要打开来历不明的文件和邮件，不随便共享文件。

3.8 定期升级操作系统的安全补丁和更新，并且要安全重要补丁，可以杜绝一些后门和漏洞，减少被攻击的危险。

3.9 在 Word 中将“宏病毒防护”选项打开，并打开“提示保存 Normal 模板”，退出 Word，然后将 Normal.dot 文件的属性改成只读。

3.10 在 Excel 和 PowerPoint 中将“宏病毒防护”选项打开。

3.11 若要使用 Outlook / Outlook express 收发电子函件，应关闭信件预览功能。

3.12 使用高强度的口令。尽量选择难于猜测的口令，对不同的账户选用不同的口令。

3.13 定期备份系统中重要的数据和文件。个人要做到每月备份，较大的单位要做到每周作完全备份，每天进行增量备份，并且每个月要对备份进行校验。

3.14 定期检查敏感文件。对系统的一些敏感文件定期进行检查，保证及时发现已感染的病毒和黑客程序。

综上所述，计算机病毒对计算机用户的危害是尤为严重的，必须采取行之有效的防护措施，才能确保计算机用户的安全。

参考文献

[1]殷伟.计算机安全与病毒防治[M].合肥：安徽科学技术出版社，2004.

[2]陈素然.计算机网络安全与防范技术研究[J].科技风，2009(22)：35-36.

[3] 韩薇卿. 计算机病毒分析与防范大全 [M]. 北京：电子工业出版社，2006.4.