doi: 10.3969/j.issn.1006-1576.2012.01.027

计算机病毒技术分析

刘晋辉
（中国兵器装备集团信息中心，北京 100089）

摘要：对现有的计算机病毒常用技术进行研究和分析，从计算机病毒的种类和特点入手，阐述当前计算机病毒破坏操作系统所采用的主要技术手段及造成的影响，并探讨计算机病毒检测技术的发展趋势。该研究可为计算机病毒检测提供参考。

关键词：计算机病毒；计算机网络；操作系统
中图分类号：TP393.08 **文献标志码**：A

Computer Virus Technical Analysis

Liu Jinhui
(*Information Center*, *China South Industries Group Corp*., *Beijing* 100089, *China*)

Abstract: Research and analysis of existing computer viruses commonly used technology, from the types and characteristics of computer viruses approach to explain the current computer virus destroyed the main operating system used and the impact of technological means, and to explore the computer virus detection technology trends. The study can provide a reference for computer virus detection

Key words: computer virus; computer network; operating system

0 引言

计算机病毒(computer virus，以下简称病毒)[1]是计算机技术和以计算机为核心的社会信息化进程发展到一定阶段的必然产物，是计算机犯罪的一种新的衍化形式。随着信息化技术的发展，每年因为计算机病毒造成的直接和间接的经济损失越来越大。研究、掌握计算机病毒技术内幕对清除计算机病毒具有重要的意义。因此，笔者对现有的计算机病毒技术进行研究。

1 计算机病毒的概念及分类

计算机病毒是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用并且能自我复制的一组计算机指令或者程序代码。计算机病毒具有非法性、隐蔽性、潜伏性、触发性、表现性、破坏性、传染性、针对性、变异性及不可预见性等诸多特征[2]。根据载体的不同，计算机病毒可以分为以下 6 种[3]：

1) 引导性病毒

这类病毒隐藏在硬盘或软盘的引导区，当计算机从感染了引导区病毒的硬盘或软盘启动，或当计算机从受感染的软盘中读取数据时，引导区病毒就将自己拷贝到机器内存中，并开始感染其他磁盘的引导区，或通过网络传播到其他计算机上。

2) 稳健性病毒

文件型病毒是以文件为宿主(virus host)或利用对文件的操作而加载执行的病毒。文件型病毒寄生在其他文件中，通过对代码加密或使用其他技术隐藏自身。文件型病毒劫夺用来启动主程序的可执行命令，用作运行自身的命令，然后将控制权交还给主程序。运行感染了病毒的程序文件，病毒被激活，执行大量的操作并进行自我复制，同时附着在系统其他可行性文件上伪装自身，并留下已感染标记。

3) 宏病毒

宏病毒是使用宏语言编写的程序，可以在一些数据处理系统中运行，存在于字处理文档、数据表格、数据库、演示文档等数据文件中，利用宏语言的功能将自身复制并且繁殖到其他数据文档中。

4) 脚本病毒

脚本病毒依赖特殊的脚本语言(如：VBScript、JavaScript 等)起作用，同时需要主软件或应用环境能够正确识别和翻译这种脚本语言中潜在的命令。脚本病毒在某些方面与宏病毒类似，但脚本病毒可以在多个产品环境中运行，也可以在其他所有可以识别和翻译它的产品中运行。脚本语言比宏语言更具有开放终端的趋势，这使得病毒制造者对感染脚

收稿日期：2011-09-07；**修回日期**：2011-09-23
作者简介：刘晋辉(1976—)，女，河南人，硕士，工程师，从事计算机软件理论与研究、网络安全研究。

本病毒的机器有更多的控制力。

5) 蠕虫(worm)程序

蠕虫程序是一种通过间接方式复制自身的非感染性病毒，这种程序通过网络等途径将自身全部或部分代码复制、传播给其它的计算机系统。蠕虫程序的传播速度相当惊人，带来的损失也难以弥补。

6) “特洛伊木马(Trojan)”程序

特洛伊木马程序通常是指伪装成合法软件的非感染型病毒，但它不进行自我复制。有些木马可以模拟运行环境，收集所需的信息，最常见的木马程序如试图窃取用户名和密码的登录窗口，或者试图从众多的 Internet 服务提供商(ISP)盗取用户的注册信息和账号信息。

2 计算机病毒技术现状

2.1 DOS 病毒技术[4]

DOS 病毒是指针对 DOS 操作系统开发的病毒，是最早出现、数量最多、变种也最多的计算机病毒。由于 Windows 操作系统的出现，DOS 病毒几乎绝迹。DOS 病毒大多只能在 DOS 环境下运行和感染，但某些 DOS 病毒在 Win9x 环境下仍可以进行感染活动，因此若执行染毒文件，Win9x 用户也会被感染。有相当一部分 DOS 病毒可以在 Windows 的 DOS 窗口下运行并传播。一部分 DOS 病毒在 Windows 下运行时，可以导致系统死机或程序运行异常。

目前发现的所有病毒中有一半以上都是 DOS 病毒，虽然 DOS 病毒数量众多，但是无论从破坏程度还是从传播速度上讲，都无法与诸如蠕虫、漏洞攻击类病毒相提并论。大部分 DOS 病毒都是制造者通过对公开代码进行一定变形而制作的恶作剧，这些病毒的绝大部分都是感染 DOS 可执行文件，如：exe 文件，com 文件，或者是 bat 文件等。

随着操作系统的不断改进，当今的病毒与 DOS 和 Win3.1S 时代下有所不同，引导区病毒减少了，而脚本性病毒开始泛滥。原因一是在当今的操作系统下直接改写磁盘的引导区有一定的难度，而且引导区的改动很容易被发现；二是脚本病毒以其传播效率高而且容易编写而深得病毒作者的青睐。

2.2 系统核心态病毒技术

所谓系统核心态病毒，是指工作在系统核心态的病毒，只限于保护模式操作系统。386 及以上的 CPU 实现了 4 个特权模式，其中特权级 0(Ring 0)是留给操作系统代码、设备驱动程序代码使用的，它们工作于系统核心态；而特权级 3(Ring 3)则给普通的用户程序使用，它们工作在用户态。运行于处理器核心态的代码不受任何限制，可以自由地访问任何有效地址，进行直接端口访问。而运行于用户态的代码则要受到处理器的诸多检查，只能访问映射其地址空间的页表项中规定的在用户态下可访问页面的虚拟地址，且只能对任务状态段(TSS)中 I/O 许可位图(I/O Permission Bitmap)中规定的可访问端口进行直接访问(此时处理器状态和控制标志寄存器 EFLAGS 中的 IOPL 通常为 0，指明当前可以直接 I/O 的最低权限级别是 Ring0)。

因为核心态有如此多的优势，当前的病毒采取各种办法获取 Ring0 权限，使得病毒本身能运行在核心态。病毒一般通过调用门(callgate)，中断门(intgate)，陷阱门(trapgate)，异常门(faultgate)，中断请求(IRQs)，端口(ports)，虚拟机管理器(VMM)，回调(callback)，形式转换(thunks)，设备 IO 控制(deviceIOcontrol)，API 函数(setthreadcontext)，终端 2E 服务(NTKERN.VxD)等技术获取 Ring0 权限。

2.3 驻留病毒技术

驻留病毒技术是指那些在内存中寻找合适的页面并将病毒自身拷贝到其中，且在系统运行期间能够始终保持病毒代码存在的一种技术。驻留病毒比那些直接感染(direct-action)型病毒更具隐蔽性，它通常要截获某些系统操作来达到感染传播的目的。进行了核心态的病毒可以利用系统服务来达到此目的，如 CHI 病毒通过调用一个由 VMM 导出的服务 VMMCALL_PageAllocate 在大于 0xC0000000 的地址上分配一块页面空间给病毒自身。

处于用户态的程序要想在程序退出后仍驻留部分代码于内存中似乎是不可能的，因为无论用户程序分配何种内存都将作为进程占用资源的一部分，一旦进程结束，所占资源将立即被释放。但病毒可以利用 WriteProcessMemory 来向其它进程(如 explorer.exe)的地址空间写入代码，或采取修改系统动态链接库(dll)的方法，只要被注入的进程不退出，病毒也不会退出，这样病毒就达到长期驻留内存的目的。

2.4 截获系统操作病毒技术

截获系统操作是病毒惯用的伎俩。DOS 时代如此，Windows 时代也不例外。在 DOS 下，病毒通过

在中断向量表中修改 INT21H 的入口地址来截获 DOS 系统服务(DOS 利用 INT21H 来提供系统调用，其中包括大量的文件操作)。而大部分引导区病毒会接挂 INT13H(提供磁盘操作服务的 BIOS 中断)从而取得对磁盘访问的控制。Windows 下的病毒同样找到了钩挂系统服务的办法。较典型的如 CIH 病毒就是利用了 IFSMGR.VXD(可安装文件系统)提供的一个系统级文件钩子来截获系统中所有文件操作。

2.5　加密变形病毒技术

早期病毒没有使用任何复杂的反检测技术，如果拿反汇编工具打开病毒体代码，看到的将是真正的机器码。因而可以由病毒体内某处一段机器代码和此处距离病毒入口偏移值来唯一确定一种病毒。查毒时只需要简单的确定病毒入口并在指定偏移处扫描特定代码串。这种静态扫描技术对付普通病毒是万无一失的。

随着病毒技术的发展，出现了一类加密病毒。这类病毒的特点是：其入口处具有解密子(decryptor)，而病毒主体代码被加了密。运行时首先得到控制权的解密代码将对病毒主体进行循环解密，完成后将控制权交给病毒主体，病毒主体感染文件时会将解密子、用随机密钥加密过的病毒主体和保存在病毒体内或嵌入解密子中的密钥一同写入被感染文件。由于同一种病毒的不同感染实例的病毒主体是用不同的密钥进行加密，因而不可能在其中找到唯一的一段代码串和偏移来代表此病毒的特征。但不同感染实例的解密子仍保持不变机器代码明文，只要将特征码选于此处，静态扫描技术对此类病毒还是非常有效的。

由于加密病毒还不能完全逃脱静态特征码扫描，所以病毒写作者在加密病毒的基础之上进行改进，使解密子的代码对不同感染实例呈现出多样性，这就出现了加密变形病毒。它和加密病毒非常类似，唯一的改进在于病毒主体在感染不同文件时会构造出一个功能相同但代码不同的解密子，也就是不同传染实例的解密子具有相同的解密功能但代码截然不同。比如原本一条指令完全可以拆成几条来完成，中间可能会被插入无用的垃圾代码。这样，由于无法找到不变的特征码，静态扫描技术就彻底失效了。

2.6　反跟踪/反虚拟执行病毒技术[5]

杀毒软件针对加密变形病毒的技术特征，利用软件模拟 CPU，将加密变形病毒的解密段在这个模拟的 CPU 上解释执行，然后在解密后的明文中查杀病毒的特征码。利用这种技术，加密变形的病毒难以躲避杀毒软件的查杀，因此，病毒制作者采用了如下更为先进的躲避技术：

首先是插入特殊指令技术，即在病毒的解密代码部分人为插入注入浮点，3DNOW，MMX 等特殊指令以达到反虚拟执行的目的。尽管虚拟机使用软件技术模拟 CPU 的工作过程，它毕竟不是真正的 CPU，由于精力有限，虚拟机的编码者不可能实现整个处理器指令集的支持，因而当虚拟机遇到其不认识的指令时将会立刻停止工作。

其次是入口模糊技术(EPO)，即病毒在不修改宿主原入口点的前提下，通过在宿主代码体内某处插入跳转指令来使病毒获得控制权。虚拟机扫描病毒时处于效率考虑不可能虚拟执行待查文件的所有代码，通常的做法是：扫描待查文件代码入口，假如在规定步数中没有发现解密循环，则由此判定该文件没有携带加密变形病毒。这种技术之所以能起到反虚拟执行的作用，在于它正好利用了虚拟机的这个假设：由于病毒是从宿主执行到一半时获得控制权的，所以虚拟机首先解释执行的是宿主入口的正常程序，当然在规定步数中不可能发现解密循环，因而产生漏报。如果虚拟机能增加规定步数的大小，则很可能随着病毒插入的跳转指令跟踪进入病毒的解密子，但确定规定步数大小很难：太大则将无畏增加正常的检测实践，太小则容易产生漏报。

另外还有多线程技术，即病毒在解密部分入口主程序中又启动了例外的工作线程，并且将真正的循环解密代码放置于工作线程中运行。由于多线程间切换调度由操作系统负责管理，而虚拟机只能在假定被执行线程独占处理器时间，即保证永远不会被抢先的前提下进行。如此一来，虚拟机对于模拟启用多线程工作的代码将很能做到与真实效果一致。多线程和结构化异常处理两种技术都利用了特定的操作系统机制来达到反虚拟执行的目的。

最后是多态技术(MetaPolymorphy)，即病毒中并非是多形的解密子加密的病毒体结构，而整体均采用变形技术。这种病毒整体都在变，没有所谓“病毒体原文”。

2.7　病毒隐藏技术

任何病毒都希望在被感染的计算机中隐藏起来不被发现，这样病毒才能实现其破坏行为。实现进程或模块隐藏应该是一个成功病毒所必须具备的特

征。为了达到这个目的，许多病毒使用了各种不同的技术来躲避杀毒软件的监测。

一个最常用最知名的技术被称为“秘密行动”法，这个技术的关键就是把病毒留下的有可能被立即发现的痕迹掩盖掉。这些痕迹包括被感染文件莫名其妙增大或者文件建立时间的改变等。由于它们太明显，很容易被用户发现，所以很多病毒的制造者都会使用一种技术来截获从磁盘上读取文件的服务程序，通过这种技术就能使得已被改动过的文件大小和创建时间看上去与改动前的一样，这样就能骗过使用者，使得他们放松警惕。

在“秘密行动”法问世以后，由于常驻内存杀毒软件的出现，一种名为“钻隧道”的方法被开发出来。常驻内存杀毒软件能防止病毒对计算机的破坏，它们能阻止病毒向磁盘的引导区和其他敏感区写入数据，以及实施对应用程序的修改和格式化硬盘等破坏活动。而“钻隧道”法能直接取得并使用为系统服务的原始文件地址，由此绕开常驻内存的杀毒软件过滤器，这种病毒感染文件的时候就不会被杀毒软件发现。

3 计算机病毒的发展趋势

随着计算机病毒检测技术的不断发展，计算机病毒也出现新的发展趋势，主要表现为：

1) 病毒传播方式不再以存储介质为主要的传播载体，网络成为计算机病毒传播的主要载体。

2) 传播病毒日益减少，网络蠕虫成为最主要和破坏力最大的病毒类型。当前网络应用日益广泛以后，网络蠕虫成为病毒制造者的首选，网络蠕虫不仅传播广、速度快而且编写简单。

3) 病毒与木马技术相互结合，出现带有明显病毒特征的木马或者木马特征的病毒。

4) 跨操作系统的病毒，以前的病毒只能感染同一类型操作系统，现如今，已经出现可以同时感染 Windows 操作系统、MAC 操作系统和 Linux 操作系统的病毒。

5) 手机病毒、信息家电病毒的出现，随着 WAP 和信息家电的普及，手机和信息家电逐步复杂化和智能化，同时，手机、信息家电和互联网的结合日益紧密，使得这类型的病毒出现的可能性越来越大。

4 结束语

笔者重点介绍了计算机病毒的技术内幕和病毒技术的细节，将有助于理解计算机病毒的原理，从而达到更好地消灭病毒的目的。

参考文献：

[1] 中华人民共和国公安部. 计算机病毒防治产品评级准则 [S/OL]. http://www.mps.gov.cn/cenweb/brjlCenweb/jps/common/article. jsp?infoid=ABC0000000000030728.

[2] 韩筱卿, 王建锋, 钟玮. 计算机病毒分析与防范大全 [M]. 北京: 电子工业出版社, 2006: 78-80.

[3] 金山公司. http://db.kingsoft.com/product/db2005/ol_help/Html/Duba7_5002VirusTypes.htm.

[4] 华夏黑客同盟. http://www.77169.com/Article/Class33/Class15/200503/15673.htm

[5] 张仁斌, 李钢, 侯整风. 计算机病毒与反病毒技术[M]. 北京: 清华大学出版社, 2006: 328-367.