6.5 磁盘杀手病毒

- 磁盘杀手病毒是系统引导型病毒
- 感染硬盘时把病毒程序存放在引导扇区而不是主引导扇区。
- 病毒发作时，可以删除磁盘上的所有数据，磁盘杀手由此而来。

- **6.5.1病毒的工作原理**
- 磁盘杀手病毒由三部分组成，即引导模块、传染模块、破坏模块。
- 引导模块驻留在引导扇区中，另外还有一部分与病毒程序的其他部分一起存放在磁盘上标记为坏簇的扇区中。
- 当用带毒磁盘引导系统时，引导扇区中的病毒程序首先进入内存中，获得系统的控制权。
- 病毒程序提取系统INT13H中断向量，并使系统内存总量减少8K，以保护驻留内存高端的病毒程序。
- 随后计算出内存高端段地址，将整个病毒程序移至内存高端
- 接着修改时钟中断INT8H使之计数，用作破坏模块的判断条件
- 然后修改INT13H中断向量指针，使之指向病毒程序的传染部分，完成病毒程序的激活，
- 最后执行正常的DOS引导。

- 对硬盘传染条件是读12扇区0道且不是0头，将硬盘的引导扇区内容调入内存中，检查其特定位置上是否有病毒标记，若有就退出传染模块，转向正常的INT13H中断服务；
- 否则就将病毒程序的引导部分写到引导扇区中，而把引导程序的另一部分与病毒程序的其他部分以及原引导扇区中的内容写到隐含扇区的最后5个扇区。

- 对软盘传染时，首先检查是否有病毒标记，若没有则将病毒程序的引导部分写到引导扇区中，而把引导程序的另一部分与病毒程序的其他部分共4个扇区和1个扇区的原引导扇区中的内容写到软盘中的3个连续空簇中，并标记为坏簇
- 若软盘中已有病毒，则判断与上一次读盘操作的驱动器号、磁头号、磁道号是否相同，如果不同就执行正常的INT13H 中断服务。
- 否则再判断[034F]单元值减1后是否为0，若不为0则执行正常的INT13H中断服务，
- 若为0就要置累计触发条件，然后再执行正常的INT13H中断服务。

- 病毒程序破坏模块的作用是当病毒程序记数已达48小时时，执行类似于磁盘格式化的数据销毁功能，使得磁盘无法使用，只有在重新格式化后，才能使用，但原来的信息则全部丧失。

- 6.5.2病毒的检测和消除
- 对磁盘杀手的检测比较方便，无论是软盘还是硬盘都可以借助于工具软件直接观察引导扇区内容，进行比较即可。
- 清除软盘中的病毒的方法是：从引导扇区中的病毒程序处找出存放原引导扇区内容在盘上的相对扇区号，进而读出正常引导扇区内容并写回引导扇区，然后把坏簇标志改为可用簇。
- 清除硬盘中病毒的方法是借助工具软件从隐含扇区的最后一个扇区中读出引导记录并写回到引导扇区，即可清除病毒。

6.7 黑色星期五病毒

- 黑色星期五病毒在13日且又是星期五时发作，删除磁盘上的所有被执行文件。
- 由于在西方13是一个不吉利的数字，因此对于既是13日又是星期五，就称为黑色星期五。
- 最初这种病毒出现在以色列希伯莱大学，故也称为希伯莱病毒。因为该大学位于耶路撒冷，又称为耶路撒冷病毒。

- 6.7.1黑色星期五病毒的特点
- 黑色星期五病毒是一种流行广且危害很大的恶性病毒。它是一种文件型病毒，传染对象是后缀为COM和EXE的可执行文件。
- 已感染病毒的.com文件，病毒程序位于最前端，而对于.exe文件则位于文件的后面。
- 但当运行含有病毒的文件时，最先运行的总是病毒程序，且首先获得系统的控制权。

- 感染黑色星期五病毒的文件属性和建立日期是不变的。
- 对于后缀是COM的文件，只感染一次，使其增加1813个字节，且病毒程序位于该文件的首部。
- 而对于后缀是EXE的文件，则可无限次的感染，其每次感染时都将病毒程序放在文件的尾部。
- 必须指出的是，病毒程序在对文件感染时，先是修改DOS的出错处理中断INT 24H，从而使病毒的感染过程能悄悄地进行。

- 黑色星期五病毒的破坏分为两种。
- 一种是利用所截获的INT 8H中断向量，在病毒程序内部设置计数器，

  当值为2时，在屏幕上显示“长方块”，

  若值为0时，则通过执行无用的字符循环程序来减慢系统速度。
- 另一种是日期和星期计数，当系统日历为13日且是星期五时，在系统中运行的EXE和COM文件就会被删除。

- 6.7.2病毒的工作原理
- 黑色星期五病毒包含三个模块：引导模块、传染模块和表现破坏模块。
- 运行受感染的文件时，病毒程序首先运行，对于尚未感染该病毒的系统，它将修改系统的INT 21H和INT 8H中断向量，使其指向病毒的传染模块和表现/破坏模块，并把病毒程序（约1.8KB）移到内存某个地方驻留。
- 在完成把自身引导驻留在内存的工作后才去执行原来的可执行文件。

- 在病毒处于激活状态的系统中，每运行一个文件，病毒程序将予以检查，若是已带毒的.com文件，则转向原文件开头，正常执行文件主体；若是.exe文件或是未受感染的.com文件，则保存文件的属性日期，对文件进行传染。
- 病毒传染部分将首先判断是COM文件还是EXE文件，如果是.COM文件，则判断是否有病毒标设；如果是.EXE文件则不判断病毒标设直接进行传染。
- 病毒程序还将只读文件修改为普通文件，从而实施传染。对.exe文件把病毒程序链接在文件的尾部，其中第一次感染时，将根据文件长度的不同，增加字节数在1809－1823之间，以后每次感染增加1808字节，直到程序无法运行或盘满为止。当盘空间小于2K字节时，病毒程序就不对文件感染。对.com文件则把病毒链接在文件的前头。
- 最后病毒程序把修改后的带毒文件写回磁盘，恢复文件的原有属性，完成传染模块的操作。

- 病毒的破坏模块：
- 由于病毒的引导机制已修改INT8H指向病毒程序，因此就判断时间计数是否为7F90H(约半小时左右),
- 若是则在屏幕左下角处出现一闪烁小方块，
- 若系统日期是13日星期五时，病毒将删除当前运行文件，即每运行一个文件，该文件即被删除。

- 6.7.3病毒的诊治
- 鉴别系统是否感染黑色星期五病毒方法是比较简单的。
- 对于静态病毒可检查文件是否有黑色星期五病毒程序的特征字符，.com文件特征字符在文件的前端，而.exe文件则位于文件的尾部。
- 若要检查内存中是否有病毒，则可编制一个短小的测试程序，在运行后再检查该文件长度是否增大了1800字节左右，并进一步考察该程序是否有病毒的特征字符。

- 在发现系统有病毒后，即可用无毒的系统盘重新启动系统，去掉内存中的病毒，对刚才使用过的文件检测静态病毒。
- 对染毒的.com文件可直接删去文件前部的1.8KB字节即可。
- 但清除.exe文件中的病毒程序比较麻烦。因为黑色星期五病毒对.exe文件的传染是以存储容量为限制的多次传染。传染过程是修改文件头，使之指向文件尾，而后将病毒程序链接在文件的尾部。
- 所以对.exe文件的消毒应是恢复文件头、删去文件尾的过程。这就需要正确查到病毒开始的标识串。
- 并找到在病毒程序下面的SS、SP、CS和IP值，并计算出正常文件的CS和IP这两个参数值。

6.8 瀑布病毒

- 瀑布病毒又名雨点病毒，它是一种专门攻击.com文件的文件型病毒，对感染的病毒不重复感染。
- 受感染的文件其大小增加1701字节，一些演化体为1704字节，1701/1704病毒由此而来。
- 该病毒发作时锁死键盘，屏幕上字符如同瀑布般的一个个脱落到屏幕底部，并发出响声，瀑布病毒和雨点病毒由此得名。

- 该病毒与通常的文件型病毒相比有如下特殊之处：

(1)它采用了一个数据加密算法，从而难于被检测。

(2)表现/破坏模块采取了一个复杂的激活方式。该算法涉及到许多参数，如计时器的计数值、键盘状态、硬盘数据、打印机参数、机器类型、监视器类型、有无时钟卡以及系统日期等。

- 目前瀑布病毒的各种演化体主要在增大的字节数和激活方式上作了变化。

- **6.8.1瀑布病毒的工作原理**
- **瀑布病毒由引导模块、传染模块和表现模块组成。**
- **运行带毒文件时，首先执行的是病毒的引导模块，以后传染模块由INT 21H的4B功能调用激活，而表现模块由时钟中断INT 1C激活。**
- **引导模块执行后，病毒先进行自我解密，恢复原文件（宿主文件），然后判断内存中是否已有瀑布病毒，若有则执行宿主文件；**
- **否则将病毒程序引入内存高端，修改INT 21H使之指向病毒传染块，修改INT 1CH使之指向病毒表现块，**
- **然后再执行正常文件。**

- 在加载运行文件时，若是INT 21H的4BH功能调用，则判断是否.com文件且文件长度小于63803字节，
- 如果符合就接着判断是否已感染瀑布病毒
- 如果没有感染，就把文件的前三字节放在病毒程序的数据区，然后加密包括正常文件前三字节在内的病毒程序，再把加密后的内容链接到该文件的尾部，并把原文件的前三个字节改为一条跳转到病毒引导程序的指令，
- 最后执行原INT 21H的4BH功能调用。

- 瀑布病毒只感染.com文件，但对command.com文件也传染。

瀑布病毒在传染过程中对受传染的.com文件时间不予修改，而且对写保护盘不作判断，所以在执行写保护软盘中的文件时出现写磁盘错误

- 病毒程序的表现模块是通过INT 1CH调用执行的

当内部计数器计数到一定数值时则执行表现程序，此时键盘被封锁，显示器为文本方式时，屏幕上方的字符似瀑布般地散落在屏幕下方并逐渐堆积起来，直到所有字符都落下来为止，才允许键盘输入，

但在操作一段时间，满足触发条件又会表现。

- 6.8.2瀑布病毒的诊治
- 鉴别系统是否有瀑布病毒方法是比较简单的。
- 对于静态病毒可检查文件是否有病毒程序的特征字符。
- 若要检查内存中是否有病毒，则可编制一个短小的测试程序，在运行后再检查该文件长度是否增大了1701字节左右，并进一步考察该程序是否有病毒的特征字符。

- 在发现系统有病毒后，即可用无毒的系统盘重新启动系统，去掉内存中的病毒，对刚才使用过的文件检测静态病毒。
- 如果染毒文件有正常备份文件则可用复制命令覆盖带毒文件。若无备份则清除起来就比较困难。
- 这是因为原文件前3字节与病毒程序一起被加密，因此必须对病毒主体程序和数据区解密，从而得到原文件的前3字节。注意到引导模块的工作首先是自我解密并恢复原程序，如果执行这两步后就把恢复的原程序存盘，就可得到无毒的原文件
- 可考虑如何编写程序来实现消毒，其中要注意解密过程第一个断点的设置，否则容易导致死机。

6.9 “扬基”病毒

- “扬基”(Yankee)病毒是一种攻击所有可执行文件的文件型病毒，受传染的文件其大小增加约3K，并且不会被再次感染
- 该病毒发作时会使机器奏“Yankee Dodle”的美国民歌，“扬基”(Yankee)病毒名称由此而来。
- “扬基”病毒程序编制巧妙，采用了反跟踪技术，抵抗用户的检测。

- **6.9.1“扬基”病毒的工作原理**
- **“扬基”病毒同样包含引导、传染和表现三个模块。**
- **引导模块在运行带毒程序时执行，而中断INT 21H则激活传染模块，表现模块在时钟中断INT 1CH调用时执行。**
- **引导模块执行后，先恢复宿主文件的前32个字节及其运行环境，**
- **然后判断内存是否已有“扬基”病毒，若有则执行宿主文件；否则通过修改内存控制将病毒程序引入内存高端，修改INT 21H使之指向病毒传染块，修改INT 1H用来反跟踪，修改INT 1CH使之指向病毒表现块**
- **然后再执行正常文件。**

- “扬基”病毒对文件的传染也是通过INT 21H中断的4BH功能调用来实现的。
- 被病毒程序修改后的INT 21H中断服务程序将首先判断请求中断调用的功能号，
- 若不是4BH功能调用则执行正常的INT 21H中断功能调用
- 否则判断该文件是否已感染“扬基”病毒，

  如果没有感染，就修改系统的INT 24H关键性错误处理中断，并将其屏蔽起来。然后取出该文件的属性和日期保存起来，如果不是读写属性则修改为读写属性。接着将文件头0字节起共32字节移到病毒程序的首部数据区中存放，自第A字节起到第28字节止，并移动读写指针到文件尾部，将病毒程序附在后面，然后在文件头增加跳转指令使文件的入口参数指向病毒程序的引导部分，并向盘中写回文件，恢复原来文件的属性和日期

  最后执行原INT 21H的4BH功能调用。

- “扬基”病毒的传染模块除了上面的功能外，还有一个“还原”功能。
- 它在其INT 1CH中断服务程序中设置了修改INT 1H、INT 3H中断程序的功能，一旦发现用户在跟踪病毒程序，它就退出到调用INT 1H、INT 3H程序段。
- 另外，在执行4BH功能调用时，如果发现是加载后不执行（AL寄存器值不等于零），病毒程序就认为用户可能要跟踪病毒程序，即恢复原来的程序写回操作盘上，把无毒文件调入内存，以此蒙骗用户。

- 病毒程序的表现模块是通过INT 1CH调用执行的。
- 修改后的INT 1CH中断服务程序，在被调用运行到一定次数，并满足触发条件时，即执行表现程序，此时中断系统的服务，演奏一段“Yankee Dodle”的美国乐曲，干扰系统的正常工作。

- 6.9.2“扬基”病毒的诊治
- 鉴别系统是否有“扬基”病毒方法是比较简单的。
- 对于静态病毒可检查文件是否有病毒程序的特征字符。
- 若要检查内存中是否有病毒，则可检查内存总量是否被减少了4K，也可编制一个短小的测试程序，在运行后考察该程序是否有病毒的特征字符。

- 在发现系统有病毒后，即可用无毒的系统盘重新启动系统，去掉内存中的病毒，对刚才使用过的文件检测静态病毒。
- 如果染毒文件有正常备份文件则可用复制命令覆盖带毒文件。否则可利用“扬基”病毒传染模块提供的还原程序。
- 方法是：在内存中已有“扬基”病毒的情况下，用Debug程序来加载染毒文件，再退出Debug，则染毒文件已被还原成无毒的了。
- 依此方法对所有染毒文件进行操作，最后对Debug.com本身解毒后，用无毒的系统盘重新启动系统，去掉内存中的病毒。

6.10 DIR-2病毒

- DIR-2病毒是一种文件型病毒，但是其引导和驻留方式以及传染方式与以往的文件型病毒截然不同，从某种程度上讲有点类似于引导型病毒。
- 之所以称其为文件型病毒是因为它是在被其感染的文件执行时引导进入系统中，它的传染对象也是一些在系统中的可执行文件。
- 该病毒特殊的引导方式和传染机制，标志着一种特殊类型的病毒的出现。

- DIR-2病毒的传染速度极快，它一次可传染当前操作目录下的所有满足条件的EXE型和COM型文件。
- 被传染的文件长度不象染上其它文件型病毒那样长度明显改变，而是维持原状，但文件在目录表中的首簇被修改，指向存放的病毒程序处。病毒程序体在一个磁盘上只保存一个副本，且存放在该盘的最后一簇中。
- 由于所有染毒文件的首簇均指向了存放病毒程序副本所在的簇，所以病毒程序是在执行文件时首先获得对系统的控制权。

- 它驻留内存的方式也与一般的文件型病毒不同，它是以系统设备驱动程序的形式驻留内存的。
- 由于它并不修改系统的中断向量，所以用一般的检查中断向量的方式是不能发现的
- 病毒通过修改系统中所有块设备驱动程序的入口，从而获得对系统的控制。系统中所有对块设备的驱动请求，都首先转到病毒程序的传播部分。
- 此时，病毒程序开始向外传播，传播完毕才去执行系统中的设备驱动请求。

- 被DIR-2病毒传染的系统可执行文件，只有在病毒程序已驻留在内存时才能被正确地读出，从而才能进行文件的正常拷贝。此时目标盘中也已感染上了病毒。
- 当系统处在无毒状态下进行拷贝文件时，只能拷贝出文件的一个簇的内容，其长度根据操作磁盘类型的不同而不同。由于仅复制出文件的部分内容，因此这样的文件是不能正常运行的。
- 这又是与一般的文件型病毒所不同的。

- **6.10.1 DIR-2病毒的作用机制**
- **DIR-2病毒是在染毒文件执行时进入到系统中的。由于染毒文件的首簇指向了磁盘中病毒程序所驻留的地方，因此病毒程序首先被调入内存。**
- **DIR-2病毒首次进入某一系统时，是以与驻留在内存中的正常文件相似的方式驻留内存的，但不同的是它是作为系统中新的设备驱动程序而驻留的。**
- **而且病毒程序并不修改系统的中断向量，所以用检查中断向量的方式是不能发现内存中的病毒的。**

- DIR-2病毒是通过修改系统中的块设备驱动程序的入口，来使所有对磁盘的操作请求，转到其传染模块。
- 这样，尽管病毒程序没有修改系统的任何中断向量，但仍然控制了系统的所有读写磁盘的操作。在完成病毒程序的安装后，才去加载执行原来的文件。
- 此时病毒程序会将感染病毒的文件首簇号解密，使得内存中目录项的文件首簇号指针指向原正常程序区，再利用DOS功能调用INT 21H中的4B00H加载子进程功能装入原文件，正确地加载执行。

- 由于DIR-2控制了系统中的所有读写操作，因此当它截获了有关的读写操作后，即执行病毒的传染模块。
- 此时病毒程序首先判断该文件的长度是否大于2KB，如果不满足该条件则放弃传染。
- 在向目标文件传染时，病毒程序查找操作磁盘的最后簇，将病毒程序本身写到该处，在一个磁盘上只保存一个病毒程序体。
- 然后修改该文件的首簇号，使之指向放在该磁盘最后一簇的病毒程序。

- 对文件的原簇号则通过加密处理后，放到该文件目录区的第十四到第十五字节处。
- 这样病毒程序即完成了对一个可执行文件的传染。
- 接着再按此方式在操作盘的当前目录下，继续搜索下一个传染对象，直到该目录中所有满足条件的文件都已被传染为止
- 最后在传染完毕后，才去执行系统正常的设备驱动请求。

- 6.10.2 DIR-2病毒的检测和消除
- 检测系统是否含有DIR-2病毒时，由于病毒程序是以设备驱动程序的方式驻留的，因此比较复杂
- 检查系统中程序的驻留情况，通过与系统无毒时的情况进行比较，来确定是否有病毒程序的驻留
- 检测磁盘上是否含有DIR-2病毒是比较简单的。
- 因为当磁盘上含有DIR-2病毒时，该操作盘上的最后一簇一定存放着病毒程序体，各个可执行文件的首簇均指向病毒程序体所占据的簇。用工具软件可以读出被检查盘的文件目录(FDT)表。
- 如果发现所有的.EXE文件或.COM文件的目录中，文件的起始簇号都被修改为同一值(一般为该操作盘的最后一簇)，则可断定此时该盘中文件均已被染上DIR-2病毒。

- DIR-2型病毒在传染时，只是对磁盘的文件目录表进行了修改，并不对具体的执行文件进行读写操作，所以这些文件本身的数据区内容是完好的，并没被破坏。因此消除DIR-2病毒，实质上就是恢复文件目录表中的各个可执行文件的首簇，
- 故关键问题是如何得到被加密了的原文件的起始簇号。

- 病毒程序在对文件在FDT表中的首簇号加密以前，首先计算当前盘的总簇数，并根据该盘的BPB表中的“扇区/每簇”参数，产生一个两字节的加密钥，该初始钥对于360KB软盘为FE17，对于1.2MB软盘为03EB，对于硬盘为FDAD。
- 用这个初始密钥对待传染的文件的首簇号加密。
- 在传染过程中，每查到FDT表中的一个目录项，该密钥值就循环左移一位。当遇到满足传染条件的可执行文件时，该密钥值就与该文件的首簇号进行异或运算，结果放在该文件目录项的保留区14H-15H字节处。

- 而解密的过程实际上是加密过程的逆，只是当磁盘中文件较多时，逐一恢复各文件首簇号，工作量大，易出错，从而造成文件被破坏，因此建议使用消毒软件来清除病毒

6.11 新世纪病毒

- 新世纪病毒是一种文件型与系统引导型病毒相结合的混合型病毒。
- 它于1992年初在我国发现，是一种传染范围广、危害性极大的病毒。
- 在系统时钟为5月4日时，删除当前加载执行的可执行文件，并显示字符信息“New Century of Computer Now！”这也是该病毒名称的由来。

- 新世纪病毒是一种既寄生在可执行文件中（EXE文件和COM文件）又寄生在引导扇区中的病毒。当运行染毒的可执行文件或用带毒硬盘启动时，病毒程序即被激活，掌握系统的控制权。
- 该病毒程序具有自保护能力。
- 当硬盘主引导区中染有新世纪病毒后，当用户试图向硬盘开始处的6个扇区（病毒寄生区）写入数据时，病毒程序会拒绝写入，但反馈给调用程序的出口参数仍表示写盘正确。
- 当试图读取主引导扇区内容时，病毒程序又会从0道0面2扇区读取原主引导程序备份数据，以此蒙骗用户。

- 6.11.1新世纪病毒的作用机制
- 新世纪病毒是一种既寄生在可执行文件中（EXE文件和COM文件）又寄生在引导扇区中的病毒。
- 当运行染毒的可执行文件时，病毒程序即被激活，如果内存中没有该病毒，即修改INT 13H、INT 21H和INT 08H中断向量，指向病毒程序，获得对系统的控制权，并重新申请内存空间，然后利用EXEC功能调用加载原文件，执行INT 27H中断将病毒程序驻留内存，最后执行原文件。

- 如果用染毒的硬盘启动系统，由于病毒程序在主引导扇区中，因此病毒就被激活。
- 此时病毒程序首先使基本内存容量减少4K，并把程序移到内存高端，修改INT 13H中断向量，使之指向病毒程序，掌握系统的控制权，然后才去执行正常的系统引导程序。
- 该病毒还利用修改后的INT 13H服务程序判断系统运行状态，在发现系统启动完毕，并返回DOS 提示符“>”时，再修改INT 21H中断向量，指向病毒传染和破坏程序。

- 新世纪病毒的混合型病毒的特征，决定了它的传染模块也分成两种类型。
- 当运行含有病毒的可执行文件时，若发现硬盘主引导扇区没有该病毒，即把病毒程序引导部分和主引导扇区中的分区表信息一起写入硬盘的主引导扇区，
- 将原主引导扇区内容写入硬盘0面0道2扇区，
- 将病毒程序的其他部分写入硬盘0道0面3至6扇区中。

- 另一部分是攻击后缀为EXE和COM的可执行文件。
- 由于病毒程序修改了INT 21H中断向量，通过截获DOS的EXEC文件加载子功能（4B00H）
- 每当系统加载运行可执行文件时，即保存原INT 24H向量，然后将当前执行文件属性修改为可读写属性，取文件日期保存，
- 若发现该文件无病毒标设，则将病毒程序写入到该文件中，置文件日期为原值，关闭文件并恢复原文件属性，并恢复原INT 24H向量，
- 然后执行原文件。

- 运行病毒过程实际上就是病毒的破坏过程。
- 当病毒驻留内存后，病毒程序还通过提取系统时钟，检查系统日期，如果发现是5月4日，即调表现/破坏部分，在显示信息的同时，删除当前的执行文件。

- **6.11.2新世纪病毒的检测和清除**
- **在检测和清除新世纪病毒时，应注意到它是一种混合型病毒，必须对文件和主引导扇区都进行检测和清除。**
- **如果是用硬盘启动的，则可通过检测内存容量来考察硬盘主引导扇区是否感染病毒。**
- **此外还可通过检查INT 13H、INT 21H和INT 08H中断向量，来检测内存中是否有新世纪病毒。**
- **当然更精确的方法是检测硬盘的主引导扇区内容，对可执行文件进行特征码搜索。**

- 清除内存中的病毒可以用干净的系统盘重新启动。
- 如果没有干净的系统盘，则可依次将INT 13H、INT 21H和INT 08H中断向量逐个恢复，并且应先恢复INT 08H中断向量。
- 对可执行文件中的新世纪病毒，最好用干净的原文件覆盖或用消毒软件予以清除。
- 对主引导扇区中的病毒，只要将硬盘0面0道2扇区内容写回到主引导扇区中即可。
- 当然该操作必须在内存中无病毒状态下进行。

第七章 新一代计算机病毒

- 计算机病毒的发展从九十年代中期进入了快速发展，攻击目标以Windows为主，出现了双料双重，攻击杀毒软件的，具有黑客性质的病毒

- 7.1 变形多态病毒
- 从1992年以来，出现了能在传播过程中自动修改病毒代码，改变加解密例程的变形多态病毒，给病毒的检测和清除带来新的问题。
- 变形多态病毒一般有一个变异引擎，它是一种简单的机器代码生成器，它可以根据不同机器配置、所攻击的文件情况、传染次数等修改病毒程序体代码。

- 在带毒载体被运行后，病毒程序首先被执行，掌握系统控制权，变异引擎被启动，会根据变异引擎的功能读取有关信息，遇到传染对象后生成变形病毒程序，把变形病毒体和变异引擎一起附加到传染目标上，完成一次传染。
- 如果是具有对病毒程序体加密能力的病毒，则在被加载后先进行自我解密，根据变异引擎的功能读取有关信息，在把病毒程序附加到新的目标之前，采用一个互补的加密例程来加密病毒程序，然后把新产生的解密例程与加密的病毒程序体（包括变异引擎）一起附加到传染对象上。

- 这类病毒每传染一个对象就变化一种样子，变形能力可达上千亿甚至无限，给病毒检测和清除带来一定困难。
- 这类病毒有：NATAS/4744/4746病毒，HYY/3522（福州1号变形王）、变形大玩笑JOKE和CONNIE2-台湾2号变形王等。

- **7.2 Retro病毒**
- **在生物学中，Retro病毒（逆转录酶病毒）能破坏抑制细胞变异的酶，导致肿瘤产生，**
- **因此从某种程度上讲，一方面是酶要防止肿瘤产生，而另一方面则是要产生肿瘤，而其手段则是攻击它的攻击者。**
- **计算机中的Retro病毒的目标也是如此，它的任务就是寻找反病毒程序并试图删除一些关键文件，使得反病毒程序无法检测病毒。**

- 一些反病毒程序会包括一个数据文件，这个文件中存放病毒的特征标记。

  Retro病毒的攻击手段就是删除这种病毒定义文件，从而破坏了扫描程序检测病毒的能力。

- 有些反病毒产品使用完整性检查方法来检测病毒。

  把完整性信息存放到数据库中，标识每个未感染文件的关键特征，然后把当前文件与存储在数据库中原来文件的信息核对以验证文件的完整性。

  Retro病毒就会寻找这个数据库并删除它。

- 其作用机理是：当用户配置反病毒程序来创建、维护文件数据库时，该病毒被激活，
- 当用户释放磁盘空间时即删除该数据库，而反病毒程序并不知道数据库被病毒删除。
- 因此当用完整性检查技术检测病毒时，由于发现数据库不存在，就会根据当前文件产生新的数据库，而收录的则是已感染病毒的程序的完整性信息。

- 此外还有一类病毒具有惰化反病毒软件的功能。
- 这类病毒的作用就是阻止反病毒软件更新病毒数据库。
- MTX病毒在感染了系统之后，会监视其对互联网的访问，并阻塞对可能是对反病毒服务商网站的访问，从而阻止更新病毒数据库。
- 如果原来系统中反病毒软件没有该病毒信息，那么由于无法更新反病毒软件，就不能清除该病毒。

- 还有一类病毒能够取消Office所提供的防范措施。
- 如，只要选择安全级别为中等，当文档带有宏，就会发出警告。
- 而有一类病毒则能够使得此警告功能失效，即虽然设置的是中等安全级别，但当带有宏的文档被打开时却不会发出警告，而直接打开并激活宏(病毒)
- 其原理是病毒会修改注册表

- Office对宏的访问限制及警告发出是通过注册表设置控制的。一旦病毒具有修改注册表功能，就可删除对宏访问的限制。
- Listi(Killisti)病毒就具有这样的功能。它能检查注册表的AccessVBOM键值，如果键值设置为1，表明没有限制宏的访问，病毒可以继续感染。
- 如果限制了访问，则键值大于或小于1，此时该病毒将把键值修改为1，然后调用WordBasic.FileExit命令退出Word，这是因为AccessVBOM键值修改生效必须在重启Word之后。
- 再打开带有宏的文档时，原来设定的安全级别就失效了。

- 7.3“双料”、“双重”病毒
- 所谓“双料”是指病毒既能象系统引导型病毒感染软硬盘引导区，又能象文件型病毒那样感染可执行文件。
- 所谓“双重”病毒就是指即是DOS系统病毒，又是Windows系统病毒。3783（TPVO）病毒就是这类病毒的代表。
- 3783病毒在进入内存后，病毒利用自身的反串功能，给检测病毒带来困难。
- 该病毒对软硬盘引导区的感染方式类似于系统引导型病毒的传染方式。

- 它对可执行文件的传染方式是，当目标文件头两个字节是4D5A时，则判断是DOS系统运行下的文件还是Windows系统下运行的文件？
- 并根据不同文件结构实施传染，把病毒主体链接在文件尾部，使之增加3783个字节，该病毒名由此而来。
- 3783病毒对网络系统破坏极大，会使网络系统工作不正常或瘫痪。
- 在检测和清除病毒时，要清除引导区和文件中的病毒

- **7.4 PE病毒原理**
- **Win32 PE病毒标志令病毒极度疯狂的DOS时代已经过去。**
- **病毒技术的精髓是Win32汇编**
- **Win32病毒同时也是所有病毒中数量极多，破坏性极大，技巧性最强的一类病毒。譬如FunLove、中国黑客等病毒都是属于这个范畴。**

- 7.4.1病毒的重定位
- 1.为什么要重定位
- 写正常程序的时候不用去关心变量(常量)的位置，
- 源程序在编译的时候它的内存中位置计算好了。程序装入内存时，系统不会为它重定位。需要用到变量(常量)的时候直接用变量名访问(编译后就是通过偏移地址访问)就可以。
- 病毒也要用到变量(常量)，当病毒感染HOST程序后，由于依附到HOST程序中的位置不同，病毒随着HOST载入内存后，病毒中各变量(常量)在内存中的位置自然也会随着发生变化。
- 需要重定位

- 2.如何重定位
- call指令用来调用一个子程序或用来进行跳转，
- 执行时，会先将返回地址(即紧接着call语句之后的那条语句在内存中的真正地址)压入堆栈，然后将IP置为call语句所指向的地址。
- 子程序碰到ret命令后，就会将堆栈顶端的地址弹出来，并将该地址存放在IP中，
- 主程序就可以继续执行

```
call delta      ;     执行后，堆栈顶端为delta在
                      内存中的真正地址
delta:  pop ebp ;将delta在内存中的真正地址
                      存放在ebp寄存器中
        ……
lea eax,[ebp+(offset var1-offset delta)] ;
                eax中存放着var1在内存中的真实地址
```

pop语句执行后，ebp中放的是什么？
病毒程序中标号delta处在内存中的真正地址。
如果病毒程序中有变量var1，那么该变量实际在内存中的地址是ebp+(offset var1-offset delta)，即参考量delta在内存中的地址+其它变量与参考量之间的距离=其它变量在内存中的真正地址。

- 7.4. 2.获取API函数地址
- 1.为什么要获取API函数地址
- Win32 PE病毒和普通Win32 PE程序一样要调用API函数，
- 普通的Win32 PE程序里面有引入函数表，对应了代码段中所用到的API函数在动态连接库中的真实地址。调用API函数时就可由该引入函数表找到相应API函数的真正执行地址。
- Win32 PE病毒只有一个代码段，不存在引入函数段。
- 就无法直接调用相关API函数，需要先找出API函数在相应动态链接库中的地址。

- 2.如何获取API函数地址
- 要获得API函数地址，首先要获得Kernel32的基地址。
- 介绍几种获得Kernel32基地址的方法：
- 1) 利用程序的返回地址，在其附近搜索Kernel32模块基地址
- 当系统打开可执行文件时，会调用Kernel32.dll中的CreateProcess函数；
- CreateProcess函数在完成装载应用程序后，会先将返回地址压入到堆栈顶端，然后转向执行刚才装载的应用程序。
- 当该应用程序结束后，会将堆栈顶端数据弹出放到IP中，继续执行。
- 堆栈顶端保存的数据就是在Kernal32.dll中的返回地址。
- 这个返回地址是在Kernal32.dll模块中。
- 另外PE文件被装入内存时是按内存页对齐的，只要从返回地址按照页对齐的边界一页一页地往低地址搜索，就可以找到Kernel32.dll的文件头地址，即Kernel32模块的基地址。

- 2)对相应操作系统分别给出固定的Kernel32模块的基地址
- 对于不同的windows操作系统，Kernel32模块的地址是固定的，甚至API函数的大概位置都是固定的。
- Windows 98为BFF70000,
- Windows 2000为77E80000,
- Windows XP为77E60000。
- 在得到了Kernel32的模块地址后，就可以在该模块中搜索所要的API地址。
- 对于给定的API，搜索其地址可以直接通过Kernel32.dll的引出表信息搜索，同样也可以先搜索出GetProcAddress和LoadLibrary两个API函数的地址，然后利用这两个API函数得到所需要的API函数地址。

- 7.4.3.病毒如何感染其他文件
- PE病毒常见的感染其他文件的方法是在文件中添加一个新节，然后往该新节中添加病毒代码和病毒执行后的返回Host程序的代码，并修改文件头中代码开始执行位置（AddressOfEntryPoint）指向新添加的病毒节的代码入口，以便程序运行后先执行病毒代码。
- 1)感染文件的基本步骤：
- 1．判断目标文件开始的两个字节是否为“MZ”。
- 2．判断PE文件标记“PE”。
- 3．判断感染标记，如果已被感染过则跳出继续执行HOST程序，否则继续。

- 4．获得Directory（数据目录）的个数，（每个数据目录信息占8个字节）。
- 5．得到节表起始位置。(Directory的偏移地址+数据目录占用的字节数=节表起始位置)
- 6．得到目前最后节表的末尾偏移（紧接其后用于写入一个新的病毒节）
- 节表起始位置+节的个数*(每个节表占用的字节数28H)=目前最后节表的末尾偏移。
- 7．开始写入节表
- a）写入节名（8字节）。
- b）写入节的实际字节数（4字节）。
- c）写入新节在内存中的开始偏移地址（4字节），同时计算出病毒入口位置
- 上节在内存中的开始偏移地址+（上节大小/节对齐+1）×节对齐=本节在内存中的开始偏移地址。

- d)写入本节(即病毒节)在文件中对齐后的大小。
- e) 写入本节在文件中的开始位置。
- 上节在文件中的开始位置+上节对齐后的大小=本节(即病毒)在文件中的开始位置。
- f)修改映像文件头中的节表数目。
- g)修改AddressOfEntryPoint(即程序入口点指向病毒入口位置)，同时保存旧的AddressOfEntryPoint，以便返回HOST继续执行。
- h)更新SizeOfImage(内存中整个PE映像尺寸=原SizeOfImage+病毒节经过内存节对齐后的大小)。
- i)写入感染标记。
- j)写入病毒代码到新添加的节中。
- ECX =病毒长度
- ESI =病毒代码位置(不一定等于病毒执行代码开始位置)
- EDI=病毒节写入位置
- k)将当前文件位置设为文件末尾。
- PE病毒感染其他文件的方法还可以将自己分散插入到每个节的空隙

- **7.4.4病毒如何返回到Host程序**
- **为了提高生存能力，病毒不破坏HOST程序的，将控制权交给HOST程序。**
- **如何做？**
- **病毒在修改被感染文件代码开始执行位置(AddressOfEntryPoint)时，会保存原来的值，**
- **病毒在执行完病毒代码后用一个跳转语句跳到这段代码处继续执行。**
- **病毒先作一个“现在执行程序是否为病毒启动程序”的判断，如果不是启动程序，病毒才会返回HOST程序，否则继续执行程序其它部分。**
- **启动程序是没有病毒标志的**
- **写入到被感染程序中OldEIP和目前运行的HOST程序的OldEIP是否使用了同一个变量？它们之间有什么关系吗？思考!**

7.5 CIH病毒

- 该病毒在每月的26日将显示有关信息并删除当前目录下的文件。
- 一种能破坏计算机主板的计算机病毒CIH 病毒是感染WIN95 和WIN98 可执行文件的病毒。
- CIH病毒是迄今为止发现的破坏性极强的病毒之一，它发作时不仅破坏硬盘的引导区和分区表，而且破坏计算机系统 Flash BIOS 芯片中的系统程序，导致主板损坏。
- CIH 病毒是发现的首例直接破坏计算机系统硬件的病毒。

- CIH 病毒的作用机理是利用Win95/Win98系统的VxD虚拟设备功能接管系统控制权的。传染对象是Win95 和Win98 可执行文件。
- 病毒感染文件时会查找该文件的空闲区域，它首先检测文件的头部，当发现至少有184个字节的空间时，即将本身的引导代码写入此空间，其它代码也写入该文件的空闲区域。
- 因此CIH 病毒感染长度虽然有1K字节，但由于病毒代码写入文件的空闲区，所以实际上染上病毒的文件长度并不增加，而只增加块值。
- 必须指出的是，该病毒不感染DOS和WIN3.X的文件。

- CIH 病毒发作时，利用Win95/Win98的高级电源管理功能这一VxD特点进行破坏的。
- 它随机调用内存数据，从硬盘物理最先位置开始，逐一往下写随机数据，从而覆盖硬盘主引导区和BOOT区，改写硬盘数据。
- 该病毒还会用随机数据改写部分可升级主板的Flash BIOS系统程序，导致机器无法运行。

- CIH 病毒对Flash BIOS进行操作，仅在主板和芯片允许写Flash内存时才有可能，通常用DIP开关写Flash 内存时无效，因此该病毒发作时会破坏部分可升级主板的Flash BIOS，这就是CIH病毒会破坏计算机主板的原因。
- 目前，常见的CIH病毒有1.2、1.3和1.4三种版本。1.2 版本的发作时间为每年的4月26日，1.3版是每年的6月26日，而1.4 版则是每个月的26日都会发作。
- 另外CIH 病毒的“BUG”会造成Win95 的死机。原因是病毒代码要写到文件的头部，这样有时被病毒传染的文件就不能被Win95 识别，而被系统认为是非法程序，从而造成Win95的死机。因此当机器频繁死机时，就要检查一下是否有CIH 病毒了。

- CIH 病毒的传染渠道非常多，它可以通过软件之间的相互拷贝、盗版光盘的使用及互联网等多种渠道的传播造成大面积感染。
- 目前防止该病毒破坏性的最简便方法就是利用病毒对DOS 、及WIN3.X毫无影响的特点，在病毒发作的那天，用DOS引导开机后，更改系统的时间设定，跳过病发日期。

- “CIH”病毒为文件型病毒，但由于中毒后的文件长度并不增加，故不易查觉，很容易再感染其它文件。
- 虽然可以搜寻“CIH v”字串来自我测试是否已染上病毒，但误判的机会很大，一般不容易判定哪些文件真的中毒，而且由于在搜寻过程中，等于是把每个文件都打开来看，病毒很容易传播开来，从而使原本正常的文件受到病毒感染，
- 因此最好的方法还是使用最新版本的杀病毒软件，检测和清除病毒。
- 如果CIH病毒已经发作并破坏了计算机系统，应尽快更换主板，或重写BIOS芯片，重新建立系统。

7.6宏病毒

- 1995年，首次出现了针对Word 6.0文本的宏语言病毒，
- 感染Word文本文件，在文本中加入高级语言编写的程序并且通过Word字处理系统加以传播，而不是与一般微机引导病毒或文件病毒一样通过截获系统中断及功能调用来传染软硬盘或可执行的二进制文件。

- 7.6.1宏病毒作用机制
- Word系统所编辑的文本分为两类：文档文件及模板文本（DOC及DOT），
- 其主要区别在于文档文件中仅包含了文本数据信息，如文字、字体、段落篇章格式、图像数据等，此外还记录了其对应的模板文件名，但并不包括宏代码，
- 模板中除可以包含文本信息外，还可有可执行的宏语言程序，系统是通过模板来控制文档的。

- 在Word的低版本中采用特定的宏语言设计，随后演化为Visual Basic的一个子集Word Basic，从而极大地增强了系统性能，使文本不仅是静态的，而且可以动态地执行某些程序及控制，但这同时也为宏语言病毒的存在提供了可乘之机。
- 所谓宏是定制的命令，一般来说，宏由一系列Word命令和动作组成，并且还可使用Word Basic宏语言来创建更复杂的宏。执行宏时，将这些命令或动作激活。
- 宏可以对所有的文档有效，也可以只对那些基于特定模板的文档有效。

- 打开文件的基本流程
- 打开文档时首先执行系统内部模板或当前模板的FileOpen宏，随后打开该文档后，再根据该文档所对应的模板执行AutoOpen宏，
- 但若该文件为模板文件并且携带了AutoOpen宏时，则执行该模板文件的AutoOpen宏。其它的操作过程（如存盘、打印、退出等）都有各自的宏操作相对应。

- 每个Word文档都对应一个模板，只有模板中才存放宏程序，
- 对文档进行操作时（如打开文件、关闭文件、存盘等）都是执行了相应模板中的宏程序。
- 第一，当打开一个带病毒模板后，该模板可以通过执行其中的宏程序（如AutoOpen宏）将自身所携带的病毒宏程序拷贝到Word系统中的通用模板中；
- 第二，若使用带毒模板对文件进行操作时（如存盘等），就将该文档文件重新存盘为带毒模板文件，即由原来不带宏程序的纯文本文件转换为带病毒的模板文件。
- 以上两步循环就构成宏病毒的基本传染机制。

- 感染宏病毒的现象是各不相同的，
- 如某些Office功能失效，无法保存文件，文件大小变化，文本中出现奇怪的字符串等等，
- 若怀疑有病毒，可以打开当前使用的模板，列出所有的宏程序，分析其流程进行判别。
- 不打开带毒模板则宏病毒不会传染，但因为模板文件完全可以与文档文件具有相同的文件后缀名，
- 而且现在宏病毒已不修改文件的后缀名，故通过文件后缀名判断文件类型是不可行的。
- 可通过一些常用文件操作（如打开文件、存盘等）判断文件是否带宏病毒，
- 至少可以判断是否带有宏程序，进而采取相应的处理，这是对付宏病毒的比较有效方法

7.6.2宏病毒的检测和清除

- 宏病毒传播不分操作系统，只要有应用Office系列软件的地方，都有可能传染上宏病毒，
- 大多数宏病毒都有发作日期。轻则影响计算机的正常工作，重则破坏硬盘信息，甚至格式化硬盘，危害极大。
- 宏病毒的识别是比较简单的，可用下述方法予以识别：

- 1.在使用的Word中从“工具”菜单中打开“宏”子菜单，选中“宏”命令，在打开的“宏”对话框中点中Normal模板，若发现有AutoOpen、AutoNew、AutoClose等自动宏以及FileSave、FileSaveAs、FileExit等文件操作宏或一些怪名字的宏，
- 如AAAZAO、PayLoad等，就极可能是病毒
- 因为大多数Normal模板中是不包含上述宏的。
- 但必须注意的是，由于现在一些宏病毒已具有拦截这一菜单动作的功能，有可能因此感染系统或发作，故目前来说通过“工具”菜单打开“宏”对话框有时可能是一个相当危险的动作。
- 使用Organizer来查看文档中的宏。

- 2.在使用的有关Office软件的“工具”菜单中看不到“宏”这个字；或看到“宏”但光标移到“宏”，鼠标点击两下无反映，这两种情况肯定有宏病毒。
- 3.打开一个文档，不进行任何操作，退出系统，如提示存盘，这极可能是带宏病毒，千万别存盘。
- 4.打开以DOC为后缀的文件在另存菜单中只能以模板方式存盘，也可能带有Word宏病毒。
- 5.在运行一些Office软件过程中经常出现内存不足或打印不正常，也可能有宏病毒。
- 6.在运行Word97及以上版本时，打开doc文档中出现是否启动“宏”的提示，该文档可能带有宏病毒。

- 对于早期的宏病毒用手工删除是较方便的，只需从“工具”(Tools)菜单中选择“宏”(Macro)命令列出所有宏，将模板中的病毒宏删除即可。
- 目前一些宏病毒用人工检测和消除已有一定的困难，而且有时也容易在杀毒后破坏文档，甚至无法再用WORD打开。这就需要使用针对宏病毒的杀病毒软件予以解毒，以保证杀毒后文档文件完全正常。

7.6.3典型宏病毒

- 1.台湾No.1宏病毒
- 台湾No.1宏病毒可以在Windows 3.x、Win95、Win98、Windows NT 和Mocintosh System 7等系统中传染。该病毒在每月13日发作。发作时，屏幕上出现对话框请用户计算数值，除非答对，否则将无法退出Word。而所出的题目数值是很大的。例如：
- 7003×3265×1357×48921×97=？

- 如果答错就会开出20份新文件，然后再出1道计算题，如此循环下去，不但占用内存，而且还会造成硬盘文件链的丢失
- 检测和清除该病毒的方法还是比较简单的。只要在打开的文件中检查Normal.dot中是否含有AutoOpen宏，若有按“删除”按钮就可清除该病毒，这也是对付早期宏病毒的方法，但对现在的宏病毒就不一定有效，甚至带来危险。

- 2.Cap宏病毒
- Cap宏病毒是第一个解决了SaveAs问题的宏病毒。最初的宏病毒遇到了几个比较困难的问题：
- (1)SaveAs问题。当用SaveAs指令存放文档时，感染后的文档不允许用户选择目录、途径和文件类型。这是因为宏病毒实际上是一个模板文件dot，它只能存放到Template目录里，这种现象在“另存为”时可立即发现，因此很容易暴露自己。
- (2)语言版本问题。不同语言版本Word下创建的宏病毒通常不能在其他语言版本的Word中传播。

- (3)宏病毒的生存问题。当系统中已经有了一个宏病毒，在打开的文件中又有另一种宏病毒，第二个文档中又有第三种，此时谁能生存下来了？
- 委内瑞拉的计算机病毒制作高手——Jackey解决了，制作了Cap宏病毒。
- Cap有多个加密宏：
- Cap、AutoOpen、AutoClose、AutoExec、FileNew、FileExit、FileSave、FileSaveAs和Filetemplates，
- 还有一个不加密的空宏Tools\Macro，里面以F%n的形式记录了Cap的传播次数n。

- 感染Word文档时，Cap首先改变Word中五个现有的菜单来指向病毒代码——庞大的Cap宏。它删除了所有的现有宏，还除去了Tools/Macro和Tools/Cuctoomize，并关闭了File/Templates菜单以隐藏自己的存在。

- Cap在用SaveAs存放受感染的文档时，采用了模拟功能。
- 创建一个基于受感染模板的干净文档，这样就可以选择驱动器、目录途径和格式进行存放，但存盘后即感染。
- 因此即使以.rtf格式保存，但内部还是dot，并含有病毒代码。这样便解决了因SaveAs所带来的问题。

- Cap采用一种“推断”在不同版本中相应的确定位置的方法，这使得Cap能够不依赖单一的自动宏而又能在多数语言版本中流行。
- 为了解决自身生存问题，Cap不仅不依赖自动宏传播，相反在感染了Normal.dat后，还禁止自动宏的执行，从而解决了自身的生存问题：不会被其他的宏病毒所清除，并且会清除其他的宏病毒而独占。

- 由于Cap病毒在传染时删除了所有宏，还除去了Tools/Macro和Tools/Cuctoomize，
- 因此在清除该病毒后，还要用备份或新建Normal.dot来恢复。
- 当然也可在工具栏上选择Customize，并从Menu中选择reset all，就可恢复正常，
- 当然自己定义的宏将不再存在。

- 3.Strange Days宏病毒
- Strange Days宏病毒是第一个同时感染Word和Excel的宏病毒。
- 该病毒含模块StrangeDays，包含多个宏
- AutoOpen、AutoClose、AutoExit、ToolsMacro、ToolsOptionsMacro、Filetemplates和ViewVBCode。
- 其中AutoClose和AutoExit用来感染Word，AutoOpen用来感染Excel。
- 该病毒不但可以在Word——Word和Excel——Excel，还可以交叉传染。

- 在 Word——Word 和 Excele——Excel 传染时，病毒先将其代码传递到C:\IO.SYS文件，然后写入未感染的文档或工作表
- 病毒通过 AutoClose 和 AutoExit 在退出 Word时感染文档，并利用 AutoOpen在打开工作表时传染。

- 在交叉传染时，病毒利用Word和Excel启动时从Startup目录的自动载入：
- 在 Startup 目 录 中 创 建 新 的 Normal.dot 和 Personal.xls。
- 在新创建的Normal.dot和Personal.xls中含有一段小程序作为病毒的载入体，它包括自动宏AutoOpen 、AutoClose和AutoExit，在Word和Excel启动时执行并感染Normal.dot和Personal.xls。
- 病毒载入体从C:\IO.SYS文件中读入病毒代码并写入Normal.dot或Personal.xls，然后载入体存储并退出。
- 在下次Word和Excel启动时，将载入含病毒代码的Normal.dot和Personal.xls。

- 该病毒还具有隐形和关闭Office 97的预警机制的能力。
- 这是因为它关闭了Tools/Macro、Tools/Open、File/templates和View/VBCode菜单，还关闭了VirusBasicEditor和VirusProtection选项，并改变了在system registry的VirusProtection指令。

- 4.类模块病毒
- 面向应用程序的VB版本5及以上版本可以为Office97及其版本的应用程序编写类模块
- 类模块是一种程序结构，它能创建新的对象类型(对象是一种基本程序元素，具有名字、关联属性、方法和事件），能用很少量的代码对其操作和扩展。
- 对象可以是其他的模块、文档或者图形。

- 类模块病毒利用类模块结构来实现病毒的传染
- 由于Office自带了很多内部类对象，类模块病毒就利用内部对象来完成任务。
- 如：每个Word模板包括ThisDocument的类模块，而Excel则包含一个ThisWorkbook。
- Poppy病毒是第一个类模块病毒，它能将自己的代码从它在硬盘上创建的临时文件复制到ThisDocument。
- 由于ThisDocument模块一般总与word文档相关联，不能被清除，因此一般清除此类模块病毒仅是将其中的宏清除，有可能留下隐患。

7.7 网络计算机病毒

- 大力发展网络的同时，病毒也得到大发展。
- 网络中的病毒有的仅影响系统的正常运行，但更多的病毒是恶性的，发作的现象各有千秋：有的会格式化硬盘，有的删除系统文件，有的破坏数据库。
- 由于病毒对网络的破坏性远大于单机，因此损失难以预测。

- 7.7.1网络计算机病毒的传播方式
- 计算机网络的基本构成包括网络服务器和网络节点站。
- 计算机病毒通常首先通过有盘工作站的软盘和硬盘进入网络，然后开始在网上传播。
- 其传播方式有：
- 1.病毒直接从有盘站拷贝到服务器中；
- 2.病毒先传染工作站，在工作站内存驻留，在运行网络盘内程序时再传染给服务器；

- 3.病毒先传染工作站，在工作站内存驻留，在病毒运行时直接通过映像路径传染到服务器；
- 4.如果远程工作站被病毒侵入，病毒也可能通过通讯，在数据交换时进入网络服务器。
- 一旦病毒进入文件服务器，就可通过它迅速传染到整个网络的每一台计算机。
- 对于无盘工作站来说，由于其并非真的“无盘”（它的“盘”是网络盘），当其运行网络盘上的一个带毒程序时，便会将病毒带入内存并传染给其它程序或通过映像路径传染到服务器其它文件上，

- 7.7.2几种网络计算机病毒
- **GP1和GP3病毒是早期攻击网络的病毒，流传很广，而HTML.Prepend则是前几年开始在网上传播的病毒，利用电子邮件传播病毒，更是近年来病毒传播的一大特色。**
- **1.GP1病毒**
- **GP1病毒即Get Password 1是黑色星期五病毒的变种，被特别改写为专门突破Novell网络系统安全结构的病毒。**

- GP1病毒在被加载运行后，就停留在系统的随机存储中，
- 当Novell操作系统的常驻程序IPX和NEXT被启动后，即利用INT21H中断向量的功能进行传染，该病毒会把使用者的权限改为最高权限，在Novell网络系统中快速传染。

- 2.GP3病毒
- GP3病毒是一种文件型病毒，它感染除command.com以外的所有可执行文件。
- 当运行带毒文件时，会首先调用DOS服务的F7H号功能，如果返回值为03，则说明病毒已成功进入内存。
- 这时若加载.exe文件，就将存于CS:21处的原文件头内容经调整后恢复到SS,SP,CS和IP寄存器中并执行原程序代码，
- 如果是加载.com文件，则将CS100H以及存于CS:07处的原文件长度送入堆栈并利用DOS的F6H调用功能完成原程序的加载。

- 3.HTML.Prepend病毒
- HTML.Prepend病毒通过由网络浏览器下载文档时存储于计算机中，此病毒会感染破坏HTML和HTM文档。
- 病毒是用VBScript语言编写，对IE浏览器影响较大，而对Netscape浏览器几乎没有影响。
- HTML.Prepend病毒的主要传染途径是在传送HTML和HTM文档时进行传染。
- 病毒会检测当前HTML或HTM文档所在路径下其他HTML和HTM文档是否已感染，若没有感染则会对这些文档实施传染。

- 感染HTML.Prepend病毒的HTML和HTM文档只是在这些文档的前头加了一段VBScript程序，使得对应VBScript语言的浏览器只能播放病毒预定的画面。
- 清除该病毒很简单，只要把受感染路径下所有HTML和HTM文档调出，把这些文档前段不应存在的VBScript程序删除即可
- 必须注意要对同路径下所有HTML和HTM文档作此操作，否则会自行再生。

- 作业:1.黑色星期五病毒、瀑布病毒、“扬基”病毒它们在传染机制和引导机制上有何异同点？
- 2.杀灭HTML.Prepend病毒应注意什么？为什么
- 3.PE病毒是如何获得API函数地址的