CIH病毒 计算机病毒 分析 清除 (26)

计算机科学2000Vol 27№. 5

104-105

CIH 病毒的分析与清除

Analysing CIH and Taking Precautions Against CIH

李 越 黄春雷 TP309

(北京理工大学机电工程学院 北京100081)

Abstract CIH is one of the most dangerous Conputer Virus. In order to take precautions against CIH, this paper has made a careful study on the function of CIH. We hope, through all these effort, people could find a way to protect computer away from being infeced ty CIH.

Keywords CIH, Computer virus, Analysing, Precautions

CIH是第一例感染Windows95/98环境下PE格式EXE文件的病毒,病毒发作时直接攻击和破坏计算机硬件系统。剖析CIH病毒机理,掌握在Windows平台下病毒驻留和传染方法,对于预防、检测和清除CIH病毒,乃至预防未来新型Windows病毒都具有十分重要的意义。目前CIH病毒有多个版本,本文将着重对CIHv1.2版本进行剖析。

一、病毒的运行机制

同传统的DOS型病毒相比,CIH病毒是一种文件型病毒,其宿主是Windows95/98系统下的PE格式可执行文件即EXE文件。该病毒通过文件进行传播。计算机开机以后,如果运行了带病毒的文件,其病毒就驻留在Windows核心内存里了。以后,只要运行了PE格式的EXE文件,这些文件就会感染上该病毒。CIH病毒提供了一种全新的病毒程序方式和方向。该病毒运行由三部分组成。

(一)CIH病毒的驻留(初始化) 由于病毒已修改了被感染文件程序的入口地址,所以首先调入内存执行的是病毒的驻留程序,其驻留主要过程有以下9个:

1. 用STDT指令取得IDT base address(中断描述符表基地址),然后把IDT的INT3的入口地址改为指向CIH自己的INT3程序入口部分;

2. 执行INT3指令,进入CIH自身的INT3入口程序,这样,CIH病毒就可以获得Windows最高级别的权限(Ring 0级),病毒在这段程序中首先检查调试寄存器DR0的值是否为0,用以判断先前是否有CIH病毒已经驻留;

3. 如果DR0的值不为0,则CIH病毒程序已驻留,则此CIH副本将恢复原先的INT3入口,然后正常退出INT3,跳到过程9;

4. 如果DR0的值为0,则CIH病毒将尝试进行驻留,首先将当前EBX寄存器的值赋给DR0寄存器,以生成驻留标记,然后调用INT20中断,使用VxD call Page Allocate系统调用,请求系统分配2个PAGE大小的Windows系统内存;

5. 如果内存申请成功,则从被感染文件中将原先分成多块的病毒代码收集起来,并进行组合后放到申请到的内存空间中;

6. 每次调用INT3中断进入CIH病毒体的INT3入口程序,调用INT20来完成调用一个IFSMgr-InstallFileSystemApiHook的子程序,用来在Windows内核的文件系统处理函数中挂接钩子,以截取文件调用的操作,这样一旦系统出现要求开启文件的调用,则CIH病毒的传染部分程序就会在第一时间截获此文件;

7. 将同时获取的Windows默认的IFSMgr-Ring0_FileIO(核心文件输入/输出)服务程序的入口地址保留在DR0寄存器中,以便于CIH病毒调用;

8. 恢复原先的IDT中断表中的INT3入口,退出INT3;

9. 根据病毒内隐藏的原文件的正常入口地址,跳到原文件正常入口,执行正常程序。

(二)病毒的感染 CIH病毒的传染部分实际上是病毒在驻留内存过程中调用Windows内核低层函数IFSMgr-InstallFileSystemApiHook函数挂接钩子时指针指示的那段程序。这段程序共586字节,感染过程如下:

1. 文件的截获。每当系统出现要求开启文件的调用时,驻留内存的CIH病毒就截获该文件,病毒调用INT20的VxD call UniToBCSPath系统功能调用取回该文件的名和路径。

2. EXE文件的判断。对该文件名进行分析,若扩展文件名不为"EXE",不传染,离开病毒程序,跳回到Windows内核的正常文件处理程序上。

3. PE格式EXE判断。当病毒确认该文件是EXE文件后,打开该文件,从该文件的MS-DOS文件头(MS-DOS MZ Header)3CH处读入PE文件头的指

针，根据该指针读入 PE 文件标识符若 Signature＝"00455000"则表明该文件是 PE 格式的可执行文件，且尚未感染，跳到过程4，对其感染；否则，认为是已感染的 PE 格式文件或该文件本身就不是 PE 格式的可执行文件，而直接跳到病毒发作模块上执行。

4. 病毒首块的寄生计算。CIH 可插入 PE 格式文件的文件头及各段中 Section，CIH 病毒的首块程序被插在 PE 文件头的自由空间内。病毒首先从文件的第86H 节处读入52H 字节，这52H 字节包含了该文件的程序入口地址文件的分区数，第一个 Section header 首址以及整个文件头大小等参数，用以计算病毒首块存放的位置和大小。通常 PE 格式文件头的大小为1024字节，经估算，若减去不占有空间，整个文件头有408-448字节的自由空间可提供给病毒使用。

在 PE 格式文件头的自由空间里，CIH 病毒首先占用了(Section 数＋1)8个字节数的空间(本文称为病毒块链表指针区)，用于存放每个病毒块的长度(每块4字节)和块程序在文件头里的首地址(每块4字节)。然后 CIH 病毒将计算出的可寄存在文件头内的病毒首块字节数，送入病毒链表指针区；修改 PE 文件头，用病毒入口地址替换 PE 文件头原文件的程序入口地址，而将原文件的入口地址保存在病毒程序的第94字节内，以供病毒执行完后回到正常文件执行上来。

由于病毒的首块部分除了病毒链表指针区外必须包括病毒的184字节驻留程序，若文件头的自由空间不足，病毒不会对该文件进行感染，只是将该文件置上已感染标志。

5. 病毒其余块的寄生计算。剩余的病毒代码是分块依次插入到各 Section 里的自由空间里的。要确定该段(Section)是否有自由空间，可通过察看段首里的参数确定。病毒将整个 Section Headers 读入内存，取第一个 Section Header，计算出该 Section 的自由空间(＝PhysSize VirtSize)，以确定可存放到该区的病毒块字节数；计算出病毒块在该区的物理存放位置(＝Physoff＋VirtSize)；计算出病毒块在该文件的逻辑存放位置(＝VirtSize＋RVA＋ImageBase)；修改 VirtSize(＝该块病毒长度＋原 VirtSize)；修改 Flags 置该区为已初始化数据区和可读标志；将该区的病毒块长度和逻辑指针参数写入病毒链表指针区相应区域；求出病毒剩余长度，并取下一个 Section Header，反复前面的操作，直到病毒全部释放为止。

6. 写入病毒。病毒程序在前面只是计算出了病毒的分块、长度和插入到文件的位置等参数，将这些参数用 PUSH 指令压入栈中。在计算完所有病毒存入位置后，才进行写盘操作。写盘的步骤如下：(1)以逆序将各块病毒写入文件各区(Section)相应的自由空间中；(2)将病毒首块写入文件头自由空间内；(3)将病毒块链表指针区写入文件头；(4)将修改后的 Section Header 写回文件；(5)将修改后的 PE File Header 和 PE File Option Header 写回文件；(6)置病毒感染标志，病毒读入文件和写入文件都是通过调用系统内核的 IFSMgr_Ring0_FileIO 的读(EAX＝0000D600)和写(EAX＝0000D601)功能实现的。

(三)病毒的发作

1. 病毒发作条件判断。在 CIHv1.2中，病毒的发作日期是4月26日，病毒从 CMOS 的70、71端口取出系统当前日期，对其进行判断：如果系统当前日期不是4月26日，则离开病毒程序，回到文件的原正常操作上去；若正好是4月26日，则疯狂的 CIH 病毒破坏开始了！

2. 病毒的破坏：①通过主板的 BIOS 端口地址0CFEH 和0CFDH 向 BIOS 引导块内各写入一个字节的乱码，造成主机无法启动。所幸的是，CIH 只能对少数类型的主板 BIOS 构成威胁，因为 BIOS 的软件更新是通过直接写端口实现的，而不同主板的 BIOS 端口地址各不相同。现在出现的 CIH 只有1K，程序量太小，还不可能存储大量的主板和 BIOS 端口数据。它只对端口地址为0CFEH 和0CFDH 的 BIOS(据有关资料为 Intel 430TX chipset)进行攻击。②覆盖硬盘。通过调用 Vxd call IOS_SendCommand 直接对硬盘进行存取，将垃圾代码以2048个扇区为单位，从硬盘主引导区开始依次循环写入硬盘，直到所有硬盘(含逻辑盘)的数据均被破坏为止。

二、病毒的清除与预防

目前，检测和清除 CIH 病毒的程序已有很多，KV300、瑞星等，这些杀病毒工具都非常有效，本文只给出一般的检测和清除方法。

利用"资源管理器"进行搜寻，具体方法是：首先开启"资源管理器"，选择其中的菜单功能"工具＞查找＞文件或文件夹"，在弹出的"查找文件"设置窗口的"名称和位置"输入中输入查找路径及文件名(如：EXE)，然后在"高级＞包含文字"栏中输入要查找的特征字符串"CIH v"，最后点取"查找键"即可开始查找工作。如果在查找过程中，显示出一大堆符合查找特征的可执行文件，则表明你的计算机上已经感染了 CIH 病毒。但这种方法存在着一个致命的缺点，如果用户已感染了 CIH 病毒，那么这样大面积的搜索过程实际上也是在扩大病毒的感染面。

Debug 检测 PE Signature，用\windows\command\debug.com 检测 EXE，在 MS-DOS 方式下：

```
DEBUG XXX.EXE
-D CS:3F 41
```

如果显示的值是0x554550("UPE")，则该文件有可能已经感染了 CIH 病毒。

参 考 文 献

1 Jim Boyce，等著 Windows95高级使用指南，清华大学出版社，1996

2 木林森. Windows95使用编程与范例，清华大学出版社，1997

3 周万宁，孙抗毒. Windows95/98操作系统编程实例详解，电子工业出版社，1998