# 基于加解壳技术的防病毒保护壳

冯 敏，田继东
（西南石油大学，四川 成都 610500）

**摘 要**：计算机病毒发展日新月异，而杀毒软件的产生存在滞后性。也就是说，借助现有的杀毒软件检测系统是否感染了新现病毒是件比较棘手的事。本文基于加、解壳原理和病毒运行流程，提出了一种新的判断方法。首先对干净文件加防病毒保护壳，待运行该文件时，文件自动解壳判断是否已感染病毒，并进行相应处理，最后用 Delphi 编程实现，同时利用该 WinHex 查看加壳后的结果。实践证明，该保护壳具有可用性。

**关键词**：加、解壳原理；病毒运行流程；防病毒保护壳；Delphi
**中图分类号**：TP311.1 **文献标识码**：A

## A Protective shell based on packing/unpacking

FENG Min , TIAN Ji Dong
(Southwest Petroleum University, Chengdu 610500, China)

**Abstract** : The computer virus changes rapidly each day, while the special antivirus software has a lag. In other words, it is a more difficult thing that using the existing antivirus software testing whether system is now infected with the new virus or not. Focused on the principle of packing or unpacking and process of the virus, a new method emerged. Firstly, impose protective shell on document which is not been infected. When the document runs, the shell unpacks itself, checks if it has been infected with HIV and takes appropriate measures . Finally, make program, then show the packed document's information with WINHEX.Practice has proved that the protective shell is available. a program Take appropriate measures.

**Key words** : principle of pack/unpack; process of virus;protective shell;Delphi

自然界中植物用壳来保护种子，动物用壳来保护身体。同样，在一些计算机软件里也有一段专门负责保护软件不被非法修改或反编译的程序。它们一般都是先于程序运行，拿到控制权。就像动植物的壳一般都是在身体外面一样理所当然。从功能上看，软件的壳和自然界中的壳相差无几，无非是保护、隐蔽壳内的东西，而从技术的角度出发，壳是一段执行于原始程序前的代码。本设计所涉及的防病毒保护壳，就其本质来看就是一种“良性病毒”，它保护软件，提醒用户“可能感染了某种病毒”。

### 1 设计思路

校验法是对正常文件的内容，计算其校验和，将该校验和写入文件中或写入其他文件中保存。在文件使用过程中，定期地或每次使用文件前检查文件现在内容算出的校验和与原来保存的校验和是否一致，因而可以发现文件是否感染。但是由于病毒感染，修改了文件的某些信息，可能导致文件不能正常运行。所以，校验法仅能较好地检测病毒，而不能保护正常文件。

本文设计的防病毒保护“壳”，其基本思想和校验法相似，并在某些方面进行了改进。

防病毒保护“壳”的本质是一种良性“病毒”。它和病毒在某些方面有点类似，都在宿主程序运行之前获取控制权。但是，它对宿主程序没有破坏性。而病毒感染文件主要表现为文件的文件名、路径名或文件大小（病毒附着在被感染文件上）的改变或其他相关变化。为此，设计了一种防病毒保护壳，它能判断文件相关属性的变化，能完成自动脱“壳”功能。

### 2 具体实现步骤

当文件（PE 文件）未被感染前，就给它加防病毒

保护“壳”。

设保护壳大小 $C$，加壳标记和感染标记均为 4 个字节，加壳前文件路径和文件名为 A1、大小为 $A2$。

当运行加壳后的文件(路径和文件名为 E1、大小为 $E2$)时，若被病毒体感染，该病毒体剥离出文件(如图 1、图 2 所示)，并运行之。剥离出的文件运行时，保护壳首先获得控制权，比较 E1 与 A1,$E2$ 与($A2+C+4$)是否相等。倘若 E1 与 A1 不等，可能是某种病毒对加壳文件进行了移动操作；倘若,$E2$ 与($A2+C+4$)不等，可能是因为其他的病毒将加壳后的文件进行“包裹”，这时弹出“发现可疑病毒”；若相等，则剥离出原文件，然后创建一个新的进程运行之，运行完毕后自动终止自己。

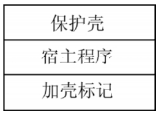


图 1 加壳后

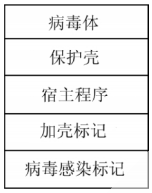


图 2 加壳之后被病毒感染

## 3 具体测试

### 3.1 防病毒保护壳测试

对“F:\calc.exe”加壳后运行。

测试中需要使用 16 进制观察器 WinHex,查看加壳后的结果。

从图 3 可以得出被加壳的文件名为 F:\calc.exe，大小为 0001C000H(即 114 688 字节)，加壳标记为 66666666H。加壳后的文件大小为 7CC6BH 字节。

```
0007CBF0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0007CC00  46 3A 5C 63 61 6C 63 2E  65 78 65 20 20 20 20 20  F:\calc.exe
0007CC10  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
0007CC20  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
0007CC30  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
0007CC40  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
0007CC50  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
0007CC60  20 20 20 20 00 C0 01 00  66 66 66 66             ....ffff
```

图 3 加壳后的文件结构

双击运行加壳后文件的截图如图 4 所示，若加壳后文件的路径、名字改变，双击运行时会提示“发现可疑病毒”，可能是被某些病毒“搬移”了。为了看到效果，我便人为地改变了加壳后的文件路径，如图 5 所示。

图 4 双击运行加壳后的 f:\calc.exe


图 5 加壳后的 f:\calc.exe 移至 f:\1 下运行

### 3.2 UPX 压缩文件测试

选用 UPX 压缩工具的主要目的是压缩防病毒保护壳（AddShell.exe）。另外，在一定程度上能保护该“壳”，防止被恶意窃取或修改。防病毒保护壳压缩前、后截如图 6、图 7 所示。图 8、图 9 分别为利用压缩后的“壳”处理文件及利用未压缩“壳”处理文件后情况。

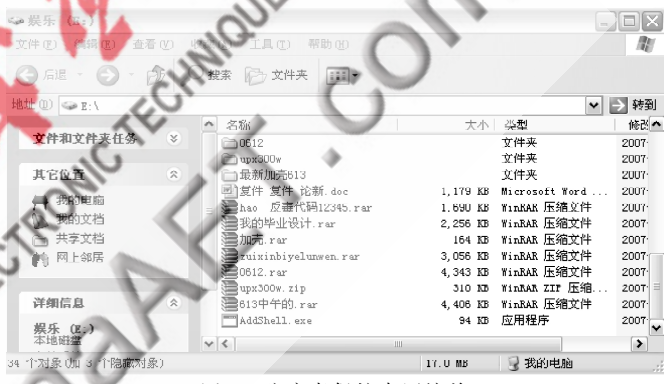

图 6 防病毒保护壳压缩前

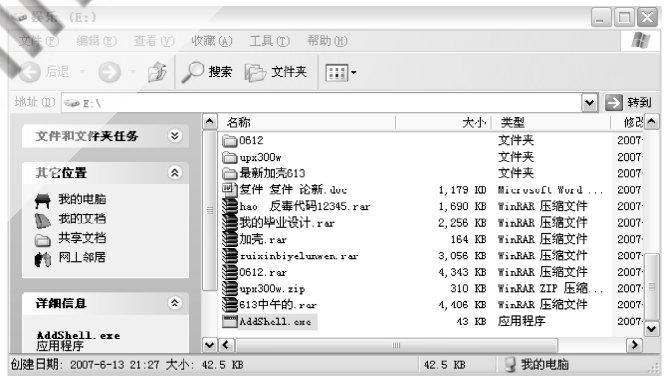

图 7 防病毒保护壳压缩后

图 8 利用压缩后的“壳”处理文件(加壳)后

图 9 未压缩的“壳”处理文件(加壳)后

从图 9 观察得出，使用未压缩壳处理 calc.exe 后文件大小为 207 KB，而使用压缩壳处理后却变为了 155 KB，达到了预期的效果。

防病毒保护壳的优点为它既可以发现已知病毒又可以发现未知病毒，在一定程度上起到保护软件不被非法修改、提醒用户及时查杀病毒等作用。

缺点是病毒感染并非文件相关信息(路径名、文件名、大小)改变的惟一的非他性原因，有可能是正常程序引起的，所以，该防病毒保护“壳”会出现误报警的情况。另外，考虑到病毒的多样性，对于出现“可疑病毒”的情况，尚未进行相应处理。

**参考文献**

[1] 陈健伟，朱梅. 计算机病毒与反病毒技术研究[J]. 电子与电信，2006, 12(34).

[2] 张桂勇，陈芳琼. APIforWindows2000/XP 详解[M]. 北京：清华大学出版社，2003.

[3] 杨华民,梁水.Delphi 函数参考大全[M]. 北京：人民邮电出版社，2006.

(收稿日期：2008-11-30)

(上接第 9 页)

发送的报文通过转发服务器转发到现场仪表中，现场仪表根据报文中的指令，返回远程 Modbus 仪表数据报文，如图 7 所示。


图 7 系统测试报文

返回的 Modbus 报文中包含了仪表采集的现场数据，可以根据这些数据进行分析，也可以把数据保存在企业现场仪表数据库中，满足企业运行的分析、决策。

通过以上对数据交互管理平台 Modbus 协议的严格测试表明：数据交互管理对 Modbus 协议能够及时快速地响应，能够响应多客户机的访问，响应时间能够在项目要求的范围内，响应数据无错误。多台客户机可以同时对数据交互管理平台进行访问，数据交互管理平台能够及时响应多台客户机的访问。

**参考文献**

[1] 刘震，徐学洲. 一种基于多级分布式管理的数据采集软件模型[J]. 现代电子技术，2003，26(19)：75-77，80.

[2] 汪奇，宋煜华. 基于B/S结构的数字视频监控系统的设计与实现[J]. 计算机工程，2006，32(19)：251-252，272.

[3] 李善平，刘文峰，王焕龙. Linux与嵌入式系统[M]. 北京：清华大学出版社，2003.

[4] 陈赜. ARM9嵌入式技术及Linux高级实践教程[M]. 北京：北京航空航天大学出版社，2005.

[5] 邹思轶. 嵌入式Linux设计与应用[M]. 北京：清华大学出版社，2002.

(收稿日期：2008-11-25)

(上接第 12 页)

用 Apriori 算法，借助于计算机，可以对于海量数据进行分析，从而可以进行更为全面和客观的预测与决策。分析的结果将会对某门课程的教学提供大量有用的信息，从而指导我们的教学。

**参考文献**

[1] 陈文伟，黄金才. 数据仓库与数据挖掘[M]. 北京：人民邮电出版社，2004.

[2] 韩家炜. 数据挖掘概念与技术[M]. 北京：机械工业出版社，2000.

[3] 齐晓峰. 数据挖掘技术在学生成绩管理中的应用研究[D]. 阜新：辽宁工程技术大学，2006.

[4] 赵辉. 数据挖掘技术在学生成绩分析中的研究及应用[D].大连：大连海事大学，2007.

[5] 陆楠. 关联规则的挖掘及其算法的研究[D]. 长春：吉林大学，2007

[6] 罗可，吴建华，吴杰. 一种用 Visual Foxpro 求频繁项目集的方法[J]. 计算机工程，2001(5).

(收稿日期：2008-11-17)