1. PE文件格式是什么？在WINDOWS系统中有哪些类型的文件属于PE文件？

PE是目前Windows平台上主流的可执行文件格式，PE文件分为几部分:DOS头、PE文件头、块表(Section Table).块(Section)、调试信息等部分。WINDOWS系统中常见的可执行程序EXE文件、动态链接库DLL文件等都是PE文件。

1. 简述WINDOWS平台下病毒运行的一般流程。

通过各种方式将自己植入内存，获取对系统的最高控制权，通过感染和嵌入正常程序达到使病毒启动的目的。

1. 简述获取PE文件中重要数据结构（数据目录表中的各个项目）的方法。

根据D0S头中的el zfanew定位延文件头的位置，再调用F文体头中的结构体变量Optonaltfader，数据目录表则是OptonalHeader中的擞组变量，根据各个项目在数据目录表中的位置（下标)获取各个项目

1. 一个程序要调用外部DLL中的函数，是直接调用这个函数吗？如果不是，是如何调用的？<http://www.doc88.com/p-102570712342.html>

不是。程序调用Loadibrary函数以在运行时加载DLL，成功加载DLL后，可以使用GetProcAddress函数获得要调用的DLL函数的地址。

5. DLL/EXE要引出一个函数给其他DLL/EXE使用，有两种实现方法。分别是什么？

DLL/EXE要引出一个函数给其他DLL/EXE使用，有两种实现方法: 通过函数名引出或者仅仅通过序数引出。比如某个DLL要引出名为"GetSysConfig"的函数，如果它以函数名引出，那么其他DLLs/EXEs若要调用这个函数，必须通过函数名，就是GetSysConfig。另外一个办法就是通过序数引出。什么是序数呢？ 序数是唯一指定DLL中某个函数的16位数字，在所指向的DLL里是独一无二的。例如在上例中，DLL可以选择通过序数引出，假设是16，那么其他DLLs/EXEs若要调用这个函数必须以该值作为GetProcAddress调用参数。这就是所谓的仅仅靠序数引出。

B19030703严妍

1、(1)PE文件分为几部分:DOS头、PE文件头、块表(Section Table).块(Section)、调试信息。(2) exe文件、dIl文件

2、通过各种方式将自己植入内存，获取对系统的最高控制权，通过感染和嵌入正常程序达到使病毒启动的目的。

3、根据D0S头中的t fanew定位延文件头的位置，再调用F文体头中的结构体变量Optonaltfader，数据目录表则是OptonalHeader中的擞组变量，根据各个项目在数据目录表中的位置（下标)获取各个项目

4、不是。程序调用Loadibrary函数以在运行时加载DLL，成功加载DLL后，可以使用GetProcAddress函数获得要调用的DLL函数的地址。

5、通过函数名引出、通过序数引出。

1.PE文件格式是什么？在WINDOWS系统中有哪些类型的文件属于PE文件？

PE是目前Windows平台上主流的可执行文件格式，PE文件分为几部分:DOS头、PE文件头、块表(SectionTable).块(Section)、调试信息等部分。WINDOWS系统中常见的可执行程序EXE文件、动态链接库DLL文件等都是PE文件。

2.简述WINDOWS平台下病毒运行的一般流程。

通过各种方式将自己植入内存，获取对系统的最高控制权，通过感染和嵌入正常程序达到使病毒启动的目的。

3.简述获取PE文件中重要数据结构（数据目录表中的各个项目）的方法。

根据DOS头中的elfanew定位延文件头的位置，再调用文体头中的结构体变量OptionalHeader，数据目录表则是OptionalHeader中的数组变量，根据各个项目在数据目录表中的位置（下标)获取各个项目

4.一个程序要调用外部DLL中的函数，是直接调用这个函数吗？如果不是，是如何调用的？http://www.doc88.com/p-102570712342.html

不是。

先调用Loadibrary函数以在运行时加载DLL，成功加载DLL后，可以使用GetProcAddress函数获得要调用的DLL函数的地址。

5.DLL/EXE要引出一个函数给其他DLL/EXE使用，有两种实现方法。分别是什么？

DLL/EXE要引出一个函数给其他DLL/EXE使用，有两种实现方法:通过函数名引出或者仅仅通过序数引出。比如某个DLL要引出名为"GetSysConfig"的函数，如果它以函数名引出，那么其他DLLs/EXEs若要调用这个函数，必须通过函数名，就是GetSysConfig。另外一个办法就是通过序数引出。什么是序数呢？序数是唯一指定DLL中某个函数的16位数字，在所指向的DLL里是独一无二的。例如在上例中，DLL可以选择通过序数引出，假设是16，那么其他DLLs/EXEs若要调用这个函数必须以该值作为GetProcAddress调用参数。这就是所谓的仅仅靠序数引出。