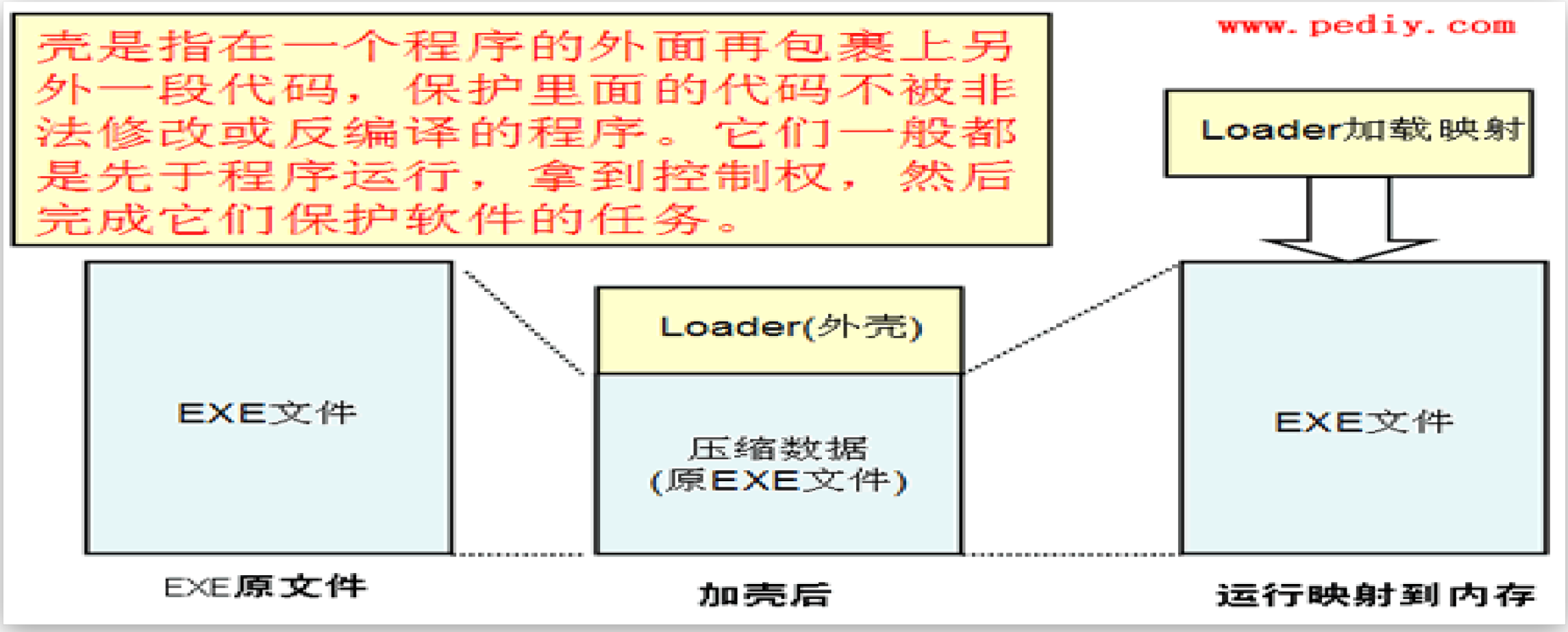
脱壳篇

什么是壳


壳是指在一个程序的外面再包裹上另外一段代码，保护里面的代码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，然后完成它们保护软件的任务。
www.pediy.com
Loader加载映射
EXE文件
Loader(外壳)
压缩数据
(原EXE文件)
EXE文件
EXE原文件
加壳后
运行映射到内存

壳的用途

- 增大逆向难度，有效防止静态分析
- 常用于病毒和木马，隐藏特征码
- 可分为：压缩壳、加密壳、虚拟机

加载过程

- **保存入口参数**
- 获取需要的API地址
- 还原文件
- **跳转到原入口点（OEP）**

脱壳

- 脱壳机自动脱壳（UPX等常见壳）
- 手动脱壳（寻找OEP）

查壳工具

- exeinfo
- Detect It Easy
- 等等

自动脱壳

工具使用，例：

```
upx -d filename
```

手动脱壳

- 单步调试法
- 堆栈平衡法

花指令篇

什么是花指令

- 在真实代码中插入一些垃圾代码的同时还保证原有程序的正确执行
- 使反汇编结果出错

花指令类型

1. 可执行式
2. 不可执行式

可执行式

UNCTF RE2

不可执行式

“ 一个必然会发生的跳转 ”

```
  xor eax, eax
  jz LABEL
  (junk data)
LABEL:
  ...
```

```
  jz LABEL
  jnz LABEL
  (junk data)
LABEL:
```

```
  call sub9
  _emit 0xE8
  jmp label9
sub9:
  add dword ptr[esp],1
  retn
label9:
```