

**恶意代码分析与防治技术课程实验报告**

**实验一**

****

学 院：网络空间安全学院

专 业：信息安全

学 号：2212998

姓 名：胡博浩

班 级：信息安全

1. **实验目的**

（1）完成教材上lab1-01至Lab1-04的题目；

（2）根据理论课要求提交所有样本在VIrusTotal和MicroSoft Defender AntiVirus上的的分析结果

1. **实验原理**
2. **PE文件格式**

PE（Portable Executable）文件是Windows操作系统下使用的一种可执行文件格式。PE文件包括以下关键部分：

1. **文件头**：存储文件的元数据，如文件类型、目标操作系统等。
2. **可选头**：包含程序入口点、堆栈大小等信息。
3. **节表**：记录程序代码、数据等的节区。
4. **导入表与导出表**：描述程序所依赖的外部DLL及导出的函数。
5. **重定位表**：确保程序在不同内存地址上运行。
6. **加壳**

加壳是将可执行文件用另一个壳程序包裹的过程，目的是增加程序的安全性、减⼩文件大小、以及防止逆向工程等恶意行为。但恶意软件经常使用加壳技术来逃避检测，增加了分析难度。

1. **实验过程**

我将使用DIE、exeinfoPE、UPX等工具来对Lab1的PE文件进行查看，分析各个样本的特征。

**（一）Lab1-01**

这个实验使用Lab01-01.exe和Lab01-01.dll文件，使用本章描述的工具和技术来获取关于这些文件的信息。

1. **将文件上传至**[**VirusTotal**](https://www.virustotal.com/)**进行分析并查看报告。文件匹配到了已有的反病毒软件特征吗？**
2. **这些文件是什么时候编译的？**
3. **这两个文件中是否存在迹象说明它们是否被加壳或混淆了？如果是，这些迹象在哪里？**
4. **是否有导入函数显示出了这个恶意代码是做什么的？如果是，是哪些导入函数？**
5. **是否有任何其他文件或基于主机的迹象，让你可以在受感染系统上查找？**

**6. 是否有基于网络的迹象，可以用来发现受感染机器上的这个恶意代码？**

**7. 你猜这些文件的目的是什么？**

**（二）Lab1-02**

分析Lab01-02.exe文件。

1. **将Lab01-02.exe文件上传至**[**VirusTotal**](https://www.virustotal.com/)**进行分析并查看报告。文件匹配到了己有的反病毒软件特征吗？**
2. **是否有这个文件被加壳或混淆的任何迹象？如果是这样，这些迹象是什么？如果该文件被加壳，请进行脱壳，如果可能的话。**
3. **有没有任何导入函数能够暗示出这个程序的功能？如果是，是哪些导入函数，他们会告诉你什么**

**4. 哪些基于主机或基于网络的迹象，可以被用来确定被这个恶意代码所感染的机器？**

1. **Lab1-03**

分析Lab01-03.exe文件。

1. **将Lab01-03.exe文件上传至**[**VIRUSTOTAL**](https://www.virustotal.com/)**进行分析并查看其反馈报告。文件匹配到了已有的反病毒软件特征吗？**
2. **是否有这个文件被加壳或混淆的任何迹象？如果是这样，这些迹象是什么？如果该文件被加壳，请进行脱壳，如果可能的话。**
3. **有没有任何导入函数能够暗示出这个程序的功能？如果是，是哪些导入函数，它们会告诉你什么？**
4. **有哪些基于主机或基于网络的迹象，可以被用来确定被这个恶意代码所感染的机器？**

**（四）Lab1-04**

分析Lab01-04.exe文件。

1. **将Lab01-04.exe文件上传至**[**VIRUSTOTAL**](https://www.virustotal.com/)**进行分析并查看其反馈报告。文件匹配到了已有的反病毒软件特征吗？**
2. **是否有这个文件被加壳或混淆的任何迹象？如果是这样，这些迹象是什么？如果该文件被加壳，请进行脱壳，如果可能的话。**
3. **这个文件是什么时候被编译的？**
4. **有没有任何导入函数能够暗示出这个程序的功能？如果是，是哪些导入函数，它们会告诉你什么？**
5. **有哪些基于主机或基于网络的迹象，可以被用来确定被这个恶意代码所感染的机器？**
6. **这个文件在资源段中包含一个资源。使用Resource Hacker工具来检查资源，然后抽取资源。从资源中你能发现什么吗？**
7. **实验结论及心得体会**

这次实验是我在恶意代码与防治分析方面的初次实践，由于本身是CTF逆向手，结合竞赛中的经验以及课堂理论和实验操作，使我对恶意代码的分析有了更深入的理解。

1. 通过实验，我对如何判断文件是否被加壳有了更全面的认识。不再仅仅依赖DIE等工具的提示，而是学会了通过对比PE文件中各节（如.text节）的虚拟大小和原始数据大小来判断是否存在加壳。

2.在分析恶意代码时，我学会了通过导入表中的特定函数来推断恶意代码的功能。例如，某些导入的函数往往与恶意行为（如文件操作、网络连接等）密切相关。并且也对VirusTotal等平台的强大功能有了直观的体会。

3.在实验中，通过使用PEview等工具，我对PE文件的结构有了更深的理解。学习了PE文件的各个组成部分，如文件头、节表、导入表等，这些信息对恶意代码的分析非常重要，特别是针对经过加壳或篡改的PE文件。