**作业1**

内容：基础题1（30%），基础题2（30%），附加题（40%）

截止时间：11月11日

**基础题1（基本分析）**

题目描述

请结合所学内容，对Lab3-1其进行基本的分析。

每个软件的分析文档需要至少包含（但不限于）：

1）使用virustotal的扫描结果（10%）

2）基本的静态分析：软件是否加壳、软件中有哪些可疑字符串需要注意、软件调用了哪些敏感API以及猜测其可能被用于做什么、在资源节中你可以得到什么提示信息等（30%）

3）基本的动态分析：软件是否进行了网络操作、软件对注册表进行了何种操作、软件执行了哪些敏感操作，从中可以提取出哪些网络、主机感染特征等（30%）

4）结合上述分析给出一个总结，描述软件的可能用途和危害。

在进行每一项分析的时候，要说明所使用的工具。如果使用的是课上内容和课本内容未涉及的工具，请给出一个工具的简单介绍（30%）

评分标准

认真完成并覆盖提到的几个点可以拿到基础分。在此基础上覆盖更多额外的方面、使用了有意思的工具会有额外加分。

提交形式

一个分析文档，命名规则：第1次作业基础题1-姓名-学号.filetype（filetype=docx、pdf……）

**基础题2（深入分析）**

题目描述

请结合所学内容，对Lab7-3进行深入的分析。你的分析报告需要包含以下几部分内容：

1）概述软件会造成的危害，尽可能做到通俗易懂（10%）

2）基本的静态分析和动态分析，截图记录必要的内容，并根据获取到的信息尝试对软件的行为做出假设（20%）

3）从IDA中记录下你认为重要的代码片段，并解释相应代码进行了何种操作（25%）

4）记录下你对软件的调试过程，以及你在调试过程中的发现和遇到的困难（25%）

5）记录用于检测恶意软件的主机、网络特征（10%）

6）对于你的分析过程做一总结（10%）

评分标准

根据各部分的完成度给出对应的分数。

提交形式

一个分析文档，命名规则：第1次作业基础题2-姓名-学号.filetype。

**附加题**

题目描述

编写代码自动玩附件中给的扫雷游戏。你编写的代码需要覆盖到以下几点：

1）显示游戏布局（15%）

2）让计时器停止（15%）

3）点到雷不会结束游戏（15%）

4）提供自动玩游戏获胜的功能（20%）

评分标准

完成相应部分可以获得对应的分数。另外，分析过程（15%）、使用手册（10%）和可用性（10%）也是评分的一部分。

提交形式

将源代码、分析文档、编译出的可执行文件和使用手册打包成一个压缩包。命名规则：第1次作业附加题-姓名-学号.zip。