# 样本分析报告

## 样本分析登记表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 样本名称 | 样本日期 | 大小(Bytes) | 样本编号 | 样本来源 |
| Lab03-03.exe | 2011.4.8 | 53,248 | 无 | Practical Malware Analysis Labs |

## 恶意代码样本分析结果登记表

|  |  |  |  |
| --- | --- | --- | --- |
| **项目** | **属性** | **详细描述** | **备注** |
| **自删除** | **无** |  |  |
| **启动方式** | **用户双击** | **双击后会拉起svchost.exe系统可执行文件** |  |
| **释放文件** | **资源文件** | **释放资源文件 异或65解密得到可执行文件** |  |
| **进程注入** | **注入进程** | **注入进程到拉起的svchost.exe** |  |
| **网络连接** | **无** |  |  |
| **其他属性** | **监听键盘事件** | **监听键盘事件并且记录相应的窗口和按键到practicalmalwareanalysis.log** |  |

## 恶意代码分析报告结构

1. 概述

该样本通过拉起svchost.exe，释放资源并且解密后注入到svchost.exe达到混淆视听的目的，其功能是通过监听键盘事件并且记录相应的窗口和按键到practicalmalwareanalysis.log来记录用户的输入

1. 行为预览
2. 恶意代码名称

Lab03-03.exe

1. 恶意代码类型

启动器

1. 恶意代码大小

53,248 bytes

1. 相关文件

practicalmalwareanalysis.log 用于记录键盘按键情况

1. 恶意代码具体行为

通过拉起svchost.exe，释放资源并且解密后注入到svchost.exe达到混淆视听的目的，其功能是通过监听键盘事件并且记录相应的窗口和按键到practicalmalwareanalysis.log来记录用户的输入

1. 加壳方式

无

1. 具体分析

见[仓库](https://github.com/papayawd/course_eyidaima)的README.md和idb文件

1. 清理方式

删除目标文件并且重启电脑