

**恶意代码课程实验报告**

**实验三：基本动态分析**

****

学 院 网络安全学院

专 业 信息安全

学 号 2110688

姓 名 史文天

班 级 1063

1. **实验目的**

**完成教材Lab3的实验内容，编写Lab3样本的Yara引擎规则，并测试规则的执行效率。**

1. **实验原理**

**配置XP虚拟机环境，安装动态、静态分析工具，使用动态分析工具。**

1. **实验过程**
2. **Lab03-01**
3. **找出这个恶意代码的导入函数与字符串列表？**

**使用PEiD打开，检测加壳信息。如图所示，可以看到壳为PEncrypt 3.1 Final -> junkcode**

**下面使用Strings查看文件的字符串，可以看到一些诸如WinVMX32、VideoDriver、vmx32to64.exe、注册表位置、注册表键值、url等信息。如下图所示。**

1. **这个恶意代码在主机上的感染迹象特征是什么？**

**打开Process Explorer，然后运行Lab03-01.exe，可以看到其对应的进程。选择查看其Handles，可以看到已经创建了互斥量WinVMX32，与字符串分析结果一致。选择查看其DLL，可以看到一些与联网功能有关的动态链接库。**

**返回Process Monitor，可以看到，此时已经监听到许多项目。进一步筛选，填入Operation is RegSetValue和Operation is WriteFile两个条件，可以检索到文件的相关操作记录。**

**点击查看相关操作记录，可以看到，文件向C:\WINDOWS\system32\vmx32to64.exe中写入了7168字节。按照其给定的路径，可以找到该文件。**

**除此之外，文件还将数据写入注册表项，命名为VideoDriver。分析可知，该文件将vmx32to64.exe写入到了开机启动的项目中。**

1. **这个恶意代码是否存在一些有用的网络特征吗？如果存在，它们是什么？**

**打开ApateDNS，可以看到恶意代码执行了DNS请求，持续访问www.praticalmalwareanalysis.com。打开WireShark可以看到，向该域名对应的服务器源源不断发送数据包。**

1. **Lab03-02**
2. **你怎样才能让这个恶意代码自行安装?**

**使用rundll32.exe Lab03-02.dll,installA或rundll32.exe Lab03-02.dll,install指令。**

1. **在安装之后，你如何让这个恶意代码运行起来？**

**使用net start IPRIP指令。**

1. **你怎么能找到这个恶意代码是在哪个进程下运行的？**

**使用Process Explorer工具，检索Lab03-02.dll，就可以看到该恶意代码是svchost.exe进程下运行。**

1. **你可以在procmon工具中设置什么样的过滤器，才能收集这个恶意代码的信息？**

**由上面分析可知，该恶意代码依附运行的进程的ID为1164，即设置PID is 1164即可收集该恶意代码的信息。**

1. **这个恶意代码在主机上的感染迹象特征是什么？**

**该恶意代码安装了IPRIP服务，并将其写入注册表，添加到开机启动项目中。**

1. **这个恶意代码是否存在一些有用的网络特征码？**

**由上面分析可知，该恶意代码对practicalmalwareanalysis.com进行了访问，并向其发送数据交互请求，使用80端口HTTP协议。做一个GET 请求，请求的资源是serve.html，使用%ComputerName% Windows XP 6.11的用户代理。**

1. **Lab03-03**
2. **当你使用Process Explorer 工具进行监视时，你注意到了什么？**

**文件运行时创建了一个子进程，接着结束掉自己的进程，留下了之前创建的子进程独立运行。**

1. **你可以找出任何的内存修改行为吗？**

**通过上述分析可知，该恶意代码将svchost.exe留下运行，而该进程在内存与磁盘中的字符串存在区别。**

1. **这个恶意代码在主机上的感染迹象特征是什么？**

**该恶意代码实现了一个键盘记录器，将键盘键入的信息保存到practicalmalwareanalysis.log文件中。**

1. **这个恶意代码的目的是什么？**

**该恶意代码利用进程替换技术，将内存中的svchost.exe进程替换成一个键盘键入记录器，将键盘键入的信息记录在了practicalmalwareanalysis.log文件中。**

1. **Lab03-04**
2. **当你运行这个文件时，会发生什么呢？**

**文件会自己删除。**

1. **是什么原因造成动态分析无法有效实施？**

**怀疑是因为缺少命令行参数或是程序内容有残缺。**

1. **是否有其他方式来运行这个程序？**

**尝试使用命令行并加入参数等方式运行程序，但依旧无法成功运行。**

1. **Yara规则**
2. **实验结论及心得体会**
3. **了解了虚拟机的安装与配置**
4. **了解并安装了多种静态和动态分析使用的工具，为后续实验打下基础。**