**恶意代码分析与防治技术实验报告**

**Lab2**

**学号：2013018 姓名：许健 专业：信息安全**

1. **实验环境**

Windows XP虚拟机、Kali虚拟机

1. **实验工具**

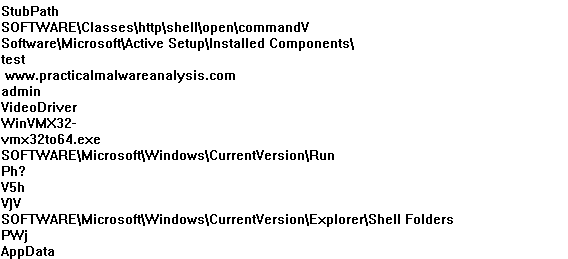
静态分析工具：PEView、PEViewer、PEiD

动态分析工具：Process Monitor、Process Explorer、Regshot、ApateDNS、INetSim、Netcat、Wireshark

善于使用虚拟机的快照功能，回到病毒分析前的状态

1. **实验内容**
2. Lab3-1
3. 找出这个恶意程序的导入函数和字符串列表？

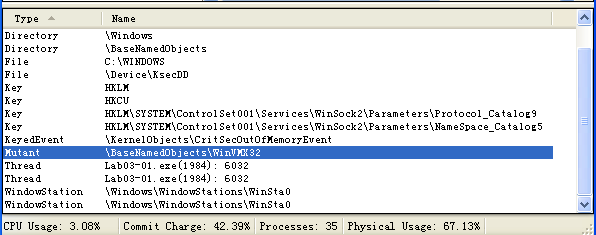
使用静态分析技术，只能看到导入函数ExitProcess，疑似被加壳，但是包含的字符串很多，包括注册表位置、域名、WinVMX32、ViedoDriver、vmx32to64exe。



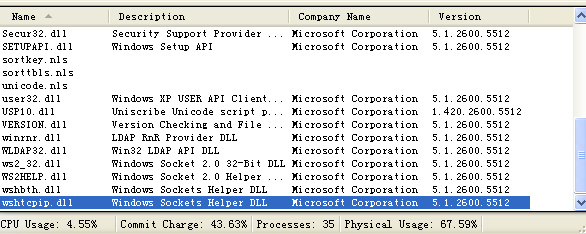
1. 这个恶意代码在主机上的感染迹象特征是什么？

我们使用动态分析，打开procmon和process explorer，同时配置出一个虚拟环境，包括ApateDNS和iNetsim，以及用于网络捕获的wireshark。

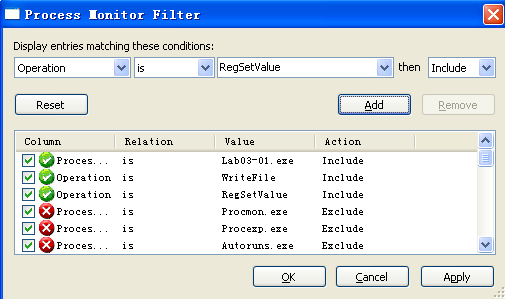
然后运行恶意程序，打开process explorer查看handles，可以看到恶意代码创建了一个名为WinVMX32的互斥量。



查看恶意代码装载的DLL文件，可以看到ws2\_32.dll和wshtcpip.dll，说明它具有联网功能。



接下来使用procmon寻找额外的信息。添加Filter，包括进程和RegSetValue、WriteFile。查看恶意代码对文件系统和注册表的修改操作。

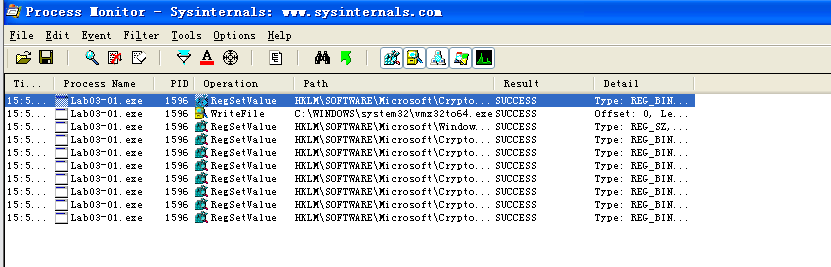


可以看到一条关于WriteFile，9条关于RegSetValue，其中\Seed上的ReGSetValue属于噪声，因为随机数发生器的种子会有软件在注册表中不断更新。

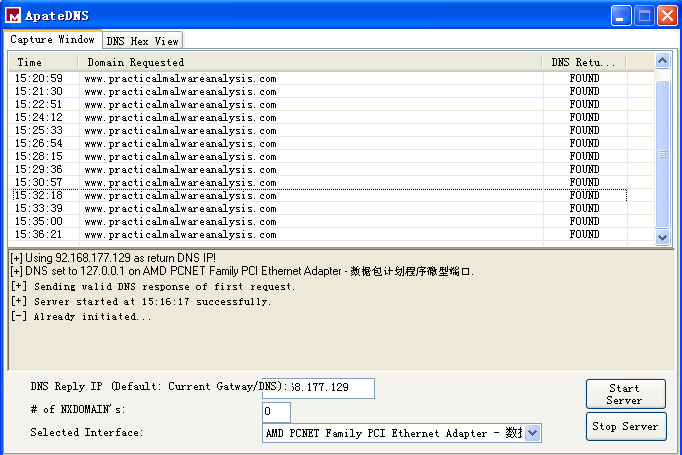
最有留下两条有趣的条目，WriteFile表示恶意代码往C:\Windows\System32\vmx32to64.exe写入7168个字节，与Lab03-01.exe大小一样，说明恶意代码将自身复制到这个文件系统位置上，属于一个有用的感染主机迹象特征。

查看注册表，可以得知恶意代码写了如下数据到注册表中，取名为VideoDriver，用于系统启动时自动运行vmx32to64.exe。

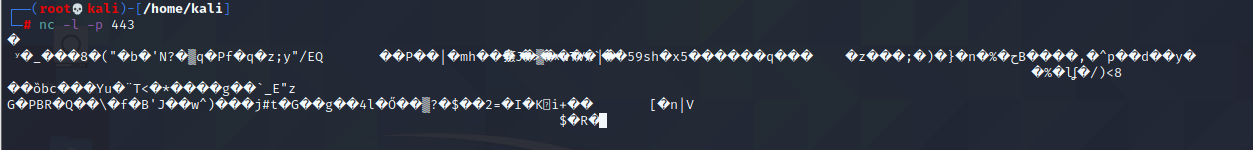
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\VideoDriver:C:\WINDOWS\system32\vmx32to64.exe



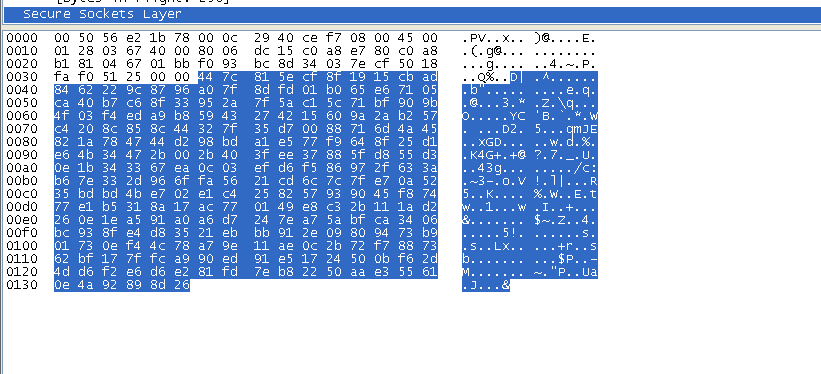
检查ApateDNS，查看恶意代码是否执行了DNS请求，通过检查输出可以看到一个对www.practicalmalwareanalysis.com域名的请求，匹配到字符串列表的显示。



检查inetsim或者netcat的结果，可以得知病毒往443端口发送了一些信号



使用wireshark抓包分析可以知道这些数据包大小是固定的256字节，看似是一些随机数据。

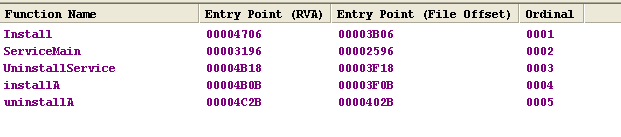


1. 这个恶意代码是否存在一些有用的网络特征码？如果存在，它们是什么？

恶意代码在进行www.practicalmalwareanalysis.com的域名解析后，持续广播大小为256字节的数据包，其中包含看似随机的二进制数据。

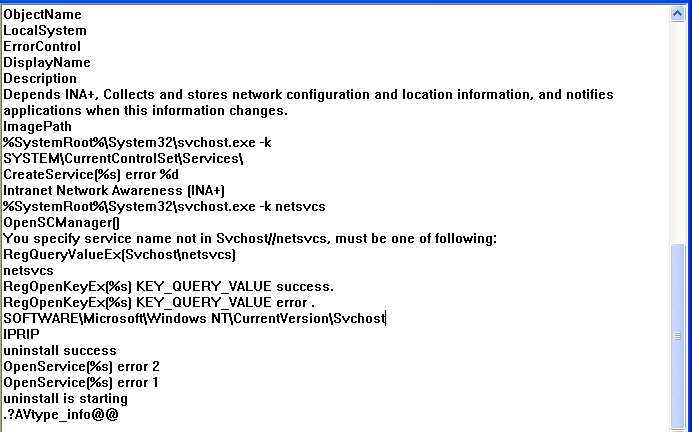
1. Lab3-2
2. 你怎样才能让这个恶意代码自行安装？

静态分析查看PE文件结构和字符串列表，该DLL含有5个导出函数，导出函数ServiceMain表明这个恶意代码需要安装成一个服务，使其能够正常运行。

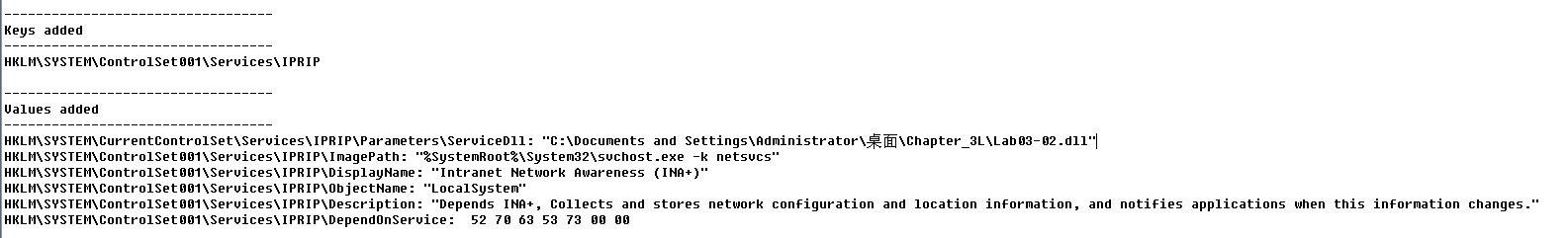


导入函数包括一些服务操作函数，比如CreateService；一些注册表操作函数比如RegSetValueEx；网络操作函数HttpSendRequest等，表示恶意代码使用了HTTP。

查看字符串列表可以看到关于注册表位置、域名等信息。



使用Regshot对注册表打快照，打开Process Explorer监视进程，使用rundll32.exe来安装恶意代码，命令为rundll32.exe Lab03-02.dll ,installA

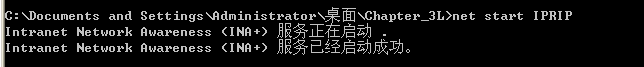


对比注册表前后变化，恶意代码将自身安装为IPRIP服务，它需要依赖可执行文件svchost.exe来执行它，说明它将会在进程svchost.exe中启动，其余信息则是恶意代码的独特指纹信息。

1. 在安装之后，你如何让这个恶意代码运行起来？

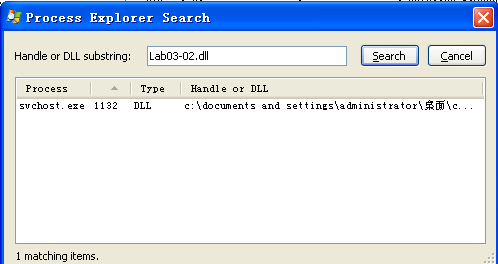
在将恶意代码安装成服务后，我们就可以启动运行它了，在此之前先打开工具、配置虚拟环境，监听80端口。

使用命令**net start IPRIP**启动它。



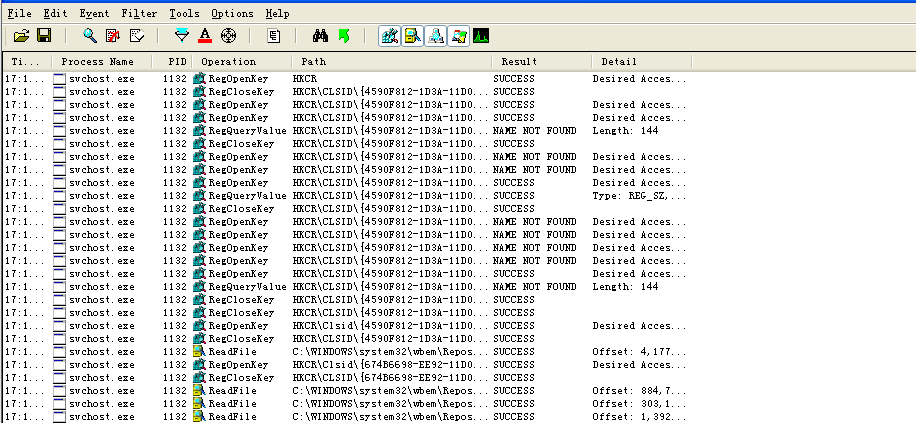
1. 你怎么找到这个恶意代码是在哪个进程下运行的？

尝试寻找出恶意代码运行的进程，使用Find Handle or DLL来查找，可以看到Lab03-02.dll由PID为1132的svchost.exe进程加载的。同时可以在服务里面找到INA+，进一步证实Lab03-02.dll被装载。



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？

使用在Process Explorer中发现的PID1132进行过滤，可以增加想监视的operation



1. 这个恶意代码在主机上的感染迹象特征是什么？

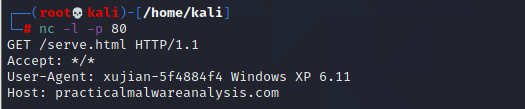
默认情况下，恶意代码安装成IPRIP服务，显示的服务名称为INA+，它会将自身持久地安装在注册表中，也就是前面在regshot中看到的项。

1. 这个恶意代码是否存在一些有用的网络特征码？

检查APateDNS可以看到恶意代码请求的DNS解析，以及使用nc监听80端口得到的数据包，恶意代码始终发送了一个对server.html的HTTP GET请求。

因此可以使用这个GET请求以及WIndows XP 6.11作为网络特征码。



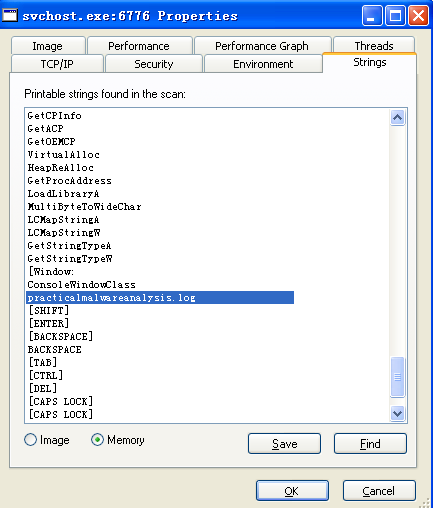


1. Lab3-3
2. 当你使用Process Explorer监视时，你注意到了什么？

开启Process Explorer和Procmon工具，运行恶意程序，在Process Explorer中可以看到恶意程序创建了svchost.exe进程后就消失了，而svchost.exe进程依然在执行且没有父进程，十分可疑，因为一般来说svchost.exe需要依赖service.exe父进程。

1. 你可以找到任何的内存修改行为吗？

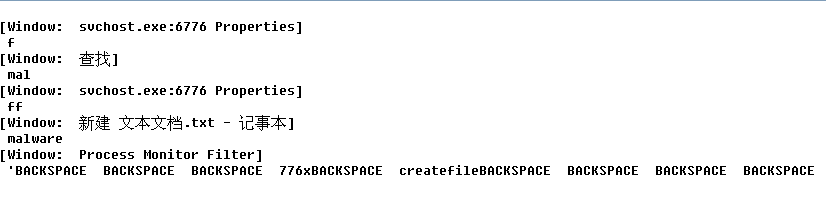
观察svchost.exe进程，查看它磁盘镜像和内存镜像中的差别，能看到在内存镜像中存在practicalmalwareanalysis.log和[ENTER]，而磁盘镜像中不会出现。



1. 这个恶意代码在主机上的感染迹象特征是什么？

猜测该程序是一个击键记录器，为了验证猜测可以打开记事本输入malware。

使用Pronmon过滤svchost.exe进程，监视CreateFile和WriteFile，可以得知进程在写practicalmalwareanalysis.log文件，打开该文件可以看到刚才输入的信息。



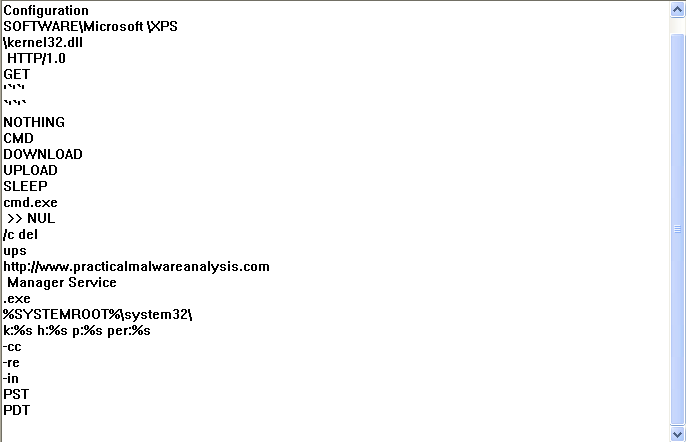
1. 这个恶意代码的目的是什么？

恶意代码是一个击键记录器，使用了svchost进程替换技术。

1. Lab3-4
2. 当你运行这个文件时，会发生什么呢？

首先执行静态分析，研究PE文件结构和字符串列表。可以知道该恶意代码导入了一些联网功能函数、服务操作函数、注册表操作函数。

在字符串列表中可以看到一些类似命令行参数的东西，以及域名、注册表位置、HTTP/1.0（恶意代码可能是一个HTTP后门程序）。



开启Pronmon和Process Explorer，配置虚拟网络，准备运行该程序。可以看到该程序运行之后很快退出，在Process Explorer中找不到有效信息。

使用Pronmon监视，可以看到一条Process Create，恶意程序通过该命令在系统中删除自身。



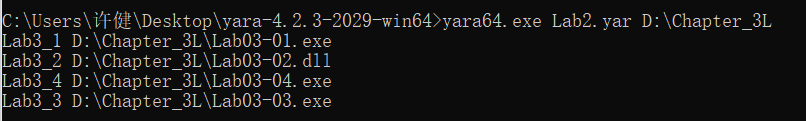
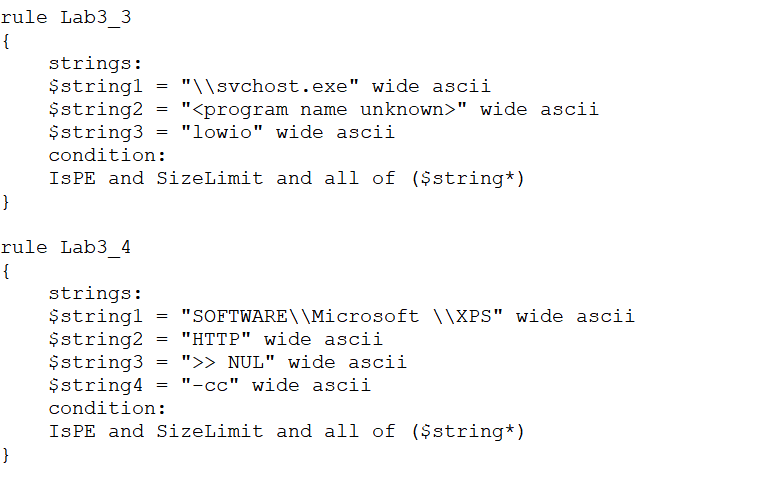
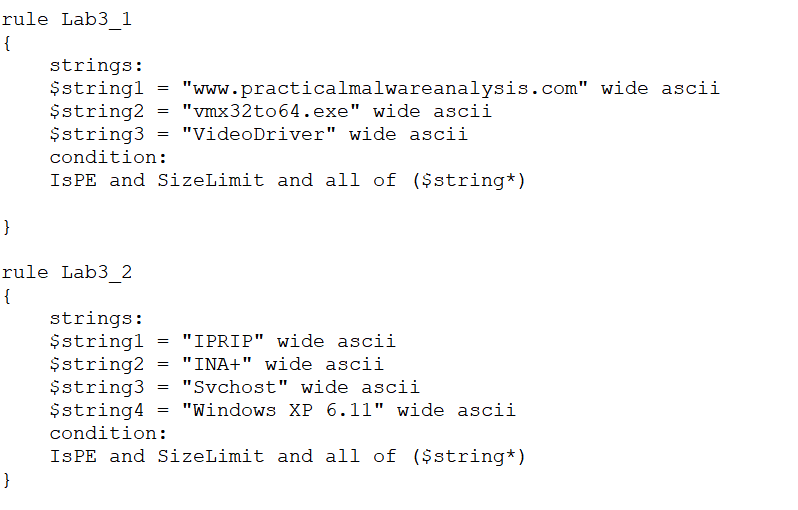
1. 是什么原因造成动态分析无法有效实施？

猜测可能需要某个命令行参数，但是尝试-cc -re -in均失败，程序依然会删除自身。

1. 是否有其他方式运行这个程序？

可以需要更加高级的动态分析工具如Ollydbg，补全缺失的部件

1. **编写Yara规则**



1. **实验心得：动态分析的优点和缺点总结**

**优点：**与静态分析相比，在动态分析程序时，分析人员需要在实际系统或仿真器中执行目标程序。通过监控运行状态和分析运行时间知识，动态分析工具可以精确检测程序错误。因此精度相对较高。

**缺点：**动态分析中目标程序的调试、分析和运行导致大量人员参与，效率低下。而且动态分析需要分析师强大的技术技能，对测试人员技术水平要求高。此外， 动态分析可伸缩性差，难以进行大规模测试等缺点。