**Lab06 – All analysis**

**1120162015 李博**

**Lab 6-1**

题目为Win32可执行程序

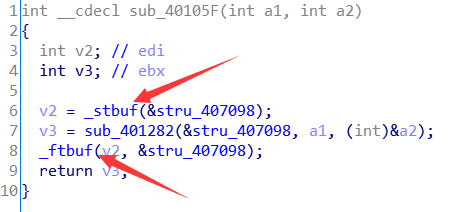
1. 

判断本地网络的连接状态，若返回不为0，表示有网络连接，否则说明无网络。



1. 

猜测是vfprintf，sub\_40105F的伪代码如下图



而原型vfprintf函数的代码如下图



并且文件流结构体的内容为

对应FILE的定义可以知道，除了文件标志符和文件描述符有值外，其它均为0，所以这个文件流应该是无效的。



1. 

该程序的目的是判断主机是否有网络连接，并将相应的字符串写入文件。但是文件流对应的内容无效（从第二题可以看到），故写文件的操作失败。

**Lab 6-2**

题目为Win32可执行程序

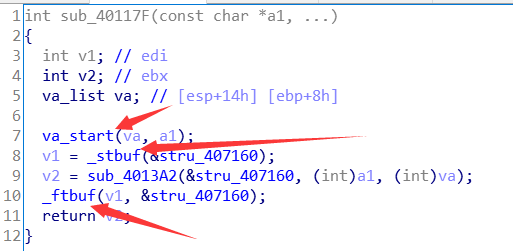
1. 

和lab 6-1的sub\_401000函数类似，获取主机的网络连接状态，并写入文件。

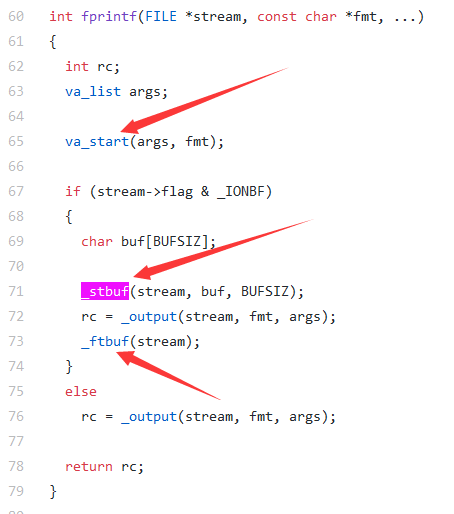
1. 

猜测是**fprintf**函数。

原函数的伪代码结构如下



而fprintf的源码如下



1. 

第二个子函数为sub\_401040。

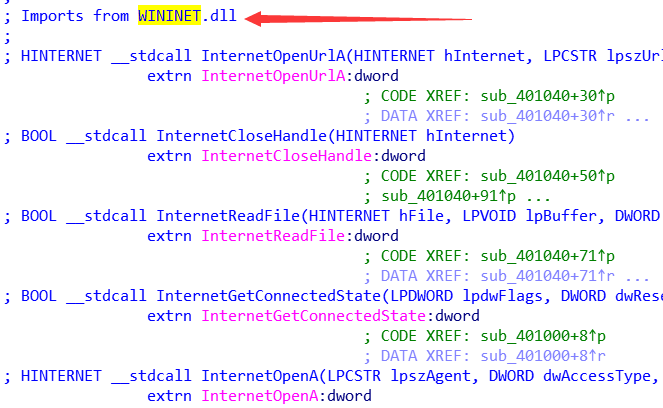
它的作用是进行网络请求，以Internet Explorer 7.5/pma为网络代理，访问并读取<http://www.practicalmalwareanalysis.com/cc.htm>，利用fprintf输出相应的字符串。

1. 

通过控制流图和汇编代码的分析，这个子函数的代码结构为if-else。



1. 
2. 引用了wininet.dll



1. 存在url和网络代理的字符串



1. 

该恶意程序的目的是判断主机网络状态，若有网络连接则访问<http://www.practicalmalwareanalysis.com/cc.htm>，读取数据。并判断数据的前四个字符是否为<!--，将第五个字符作为返回值返回。最后将第五个字符作为参数输出。

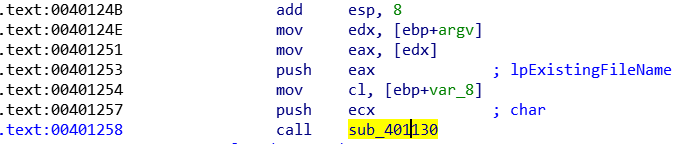
**Lab 6-3**

1. 

sub\_401130

1. 

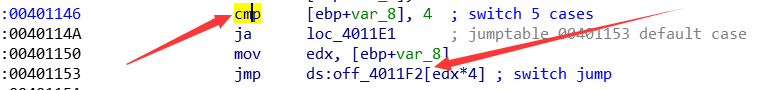
两个参数，第二个是argv[0]，即运行程序的名字，第一个是一个char类型的字符。



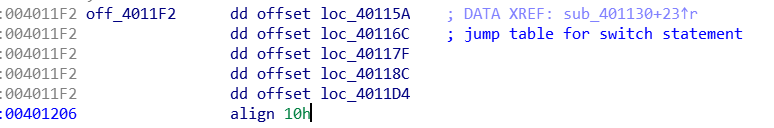
1. 

Switch结构。

如下图，首先比较var\_8和4，若var\_8大于4，则跳转至loc\_4011E1；

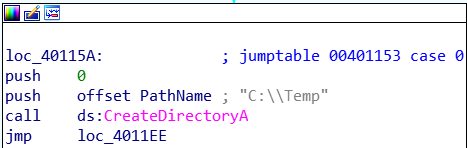


否则，将其赋值为edx，并以edx为偏移进入跳转表跳转至相应代码段。

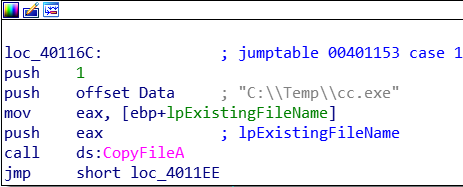


1. 

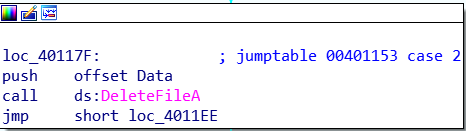
功能1：创建文件夹



功能2：复制文件



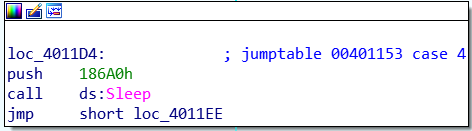
功能3：删除文件



功能4：修改注册表



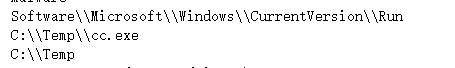
功能5：休眠100秒



1. 
2. 调用了kernel.dll



1. 存在文件路径和注册表的字符串



1. 

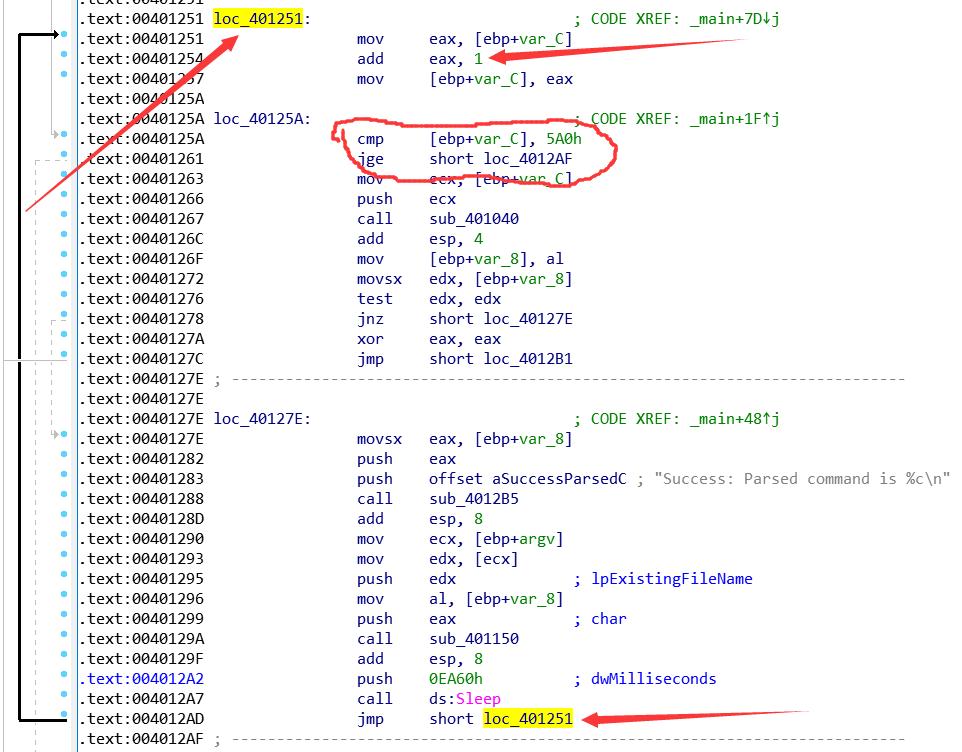
该恶意程序的目的是访问<http://www.practicalmalwareanalysis.com/cc.htm>，读取数据后判断前四个字符是否为<!--，若不是则报错。

之后以数据的第五个字符为依据，进行不同的恶意操作（创建文件夹，复制文件，删除文件，修改注册表等）。最后sleep一分钟。

**Lab 6-4**

1. 

多了一个循环操作

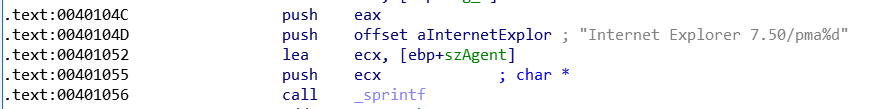


1. 

循环，同第一题。

1. 

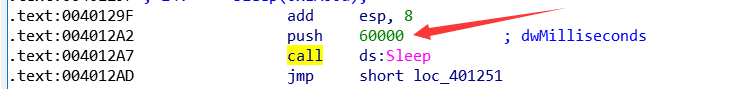
在函数sub\_401040中使用了sprintf将字符串'Internet Explorer 7.50/pma%d'赋给szAgent。



1. 

1440\*60s = 1440min = 24h

从汇编代码可以看到，每次循环sleep60秒，也就是1分钟；共进行1440次循环，故共1440分钟，即24小时。

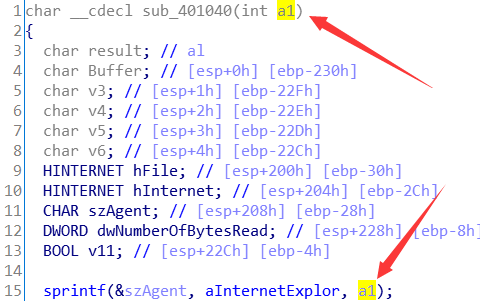
 

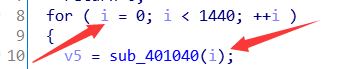
1. 

Lab 6-4: 

Lab 6-3: 

可以看到网络代理的内容发生了改变，定位至相应位置可以看到，





%d所对应的参数即表示当前运行时间。

1. 

首先获取主机的网络连接状态，若无网络则退出程序。

接着循环1440次下列操作。

将循环次数i作为参数放进代理头“Internet Explorer 7.50/pma%d”中，以此访问<http://www.practicalmalwareanalysis.com/cc.htm>并读取数据。并判断前四个字符是否为<!--，若不是则输出相应错误并返回0。若是则将第五个字符作为返回值。

接着以刚刚得到的返回值为依据，进行创建文件夹或复制文件或删除文件或修改注册表或休眠100秒的恶意操作。

最后休眠一分钟。