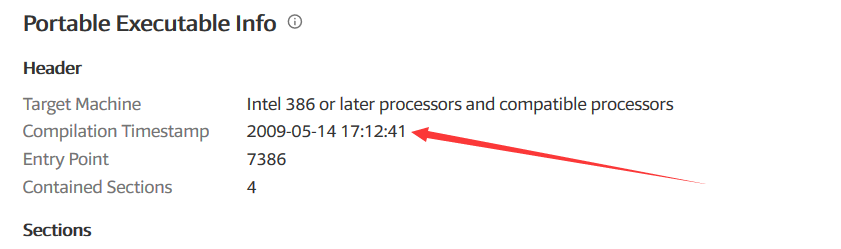
**Lab 01 ­ Basic Analysis**

**1120162015 李博**

**Lab\_01­1.malware**

1. **(1 pts) When was this file compiled?**

2009-05-14 17:12:41



**2. (6 pts) List a few imports or sets of imports and describe how the malware might use them.**

**a.    connect**，**socket**和**closesocket**三个函数。程序可能使用它们用于连接其他的服务器。

**b.    send**和**recv**这两个函数可能被用于与黑客的服务器发送和接受信息。

**c.**\_beginthread**，**CreateThread**，**ExitThread**，**GetCurrentThread函数被用于创建，销毁线程等,从而多线程处理。

**3. (6 pts) What are a few strings that stick out to you and why?**

**a.**ShellExecuteExA，cmd.exe。通过ShellExecuteExA函数可以打开文件或执行程序，将cmd.exe作为输入能执行命令行从而执行更多操作。

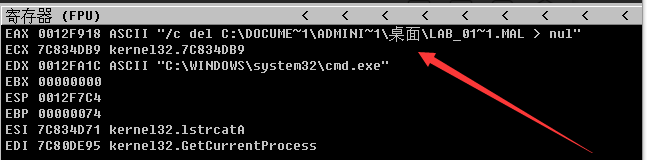
**b.** COMSPEC。因为在cmd中通过它能得到命令解释器的绝对路径名。

**c.** GetComputerNameA和GetShortPathNameA。因为通过这两个函数能获取用户主机名和路径名。

**4. (2 pts) What happens when you run this malware? Is it what you expected and why?**

该程序运行时有一点延时，之后消失。

和预期有一点不同，因为在程序执行过程中运行了cmd.exe并执行下图的shell

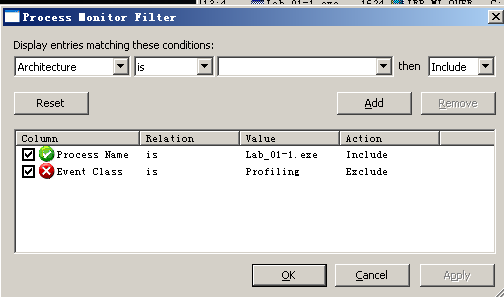


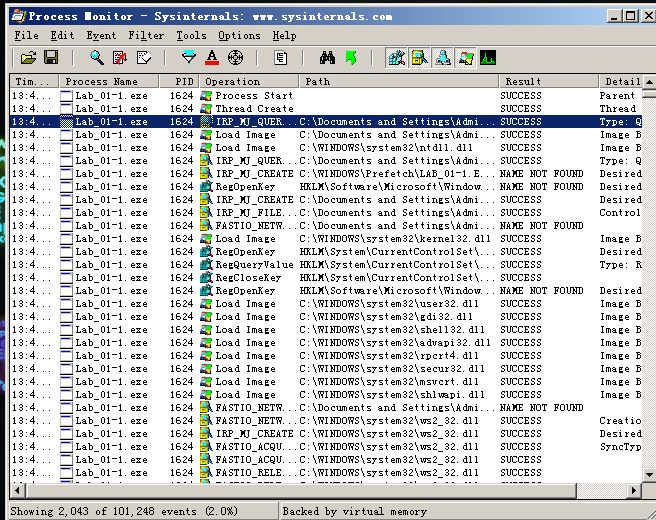
所以程序运行之后消失。

不同之处在于由于无法连接60.248.52.95，所以没有进行读写文件的操作。

**5. (2 pts) Name a procmon filter and why you used it.**

Process monitor。因为通过如下图的设置之后可以直观的看到程序进行了哪些操作。





**6. (4 pts) Are there any host­based signatures? (Files, registry keys, processes or services, etc).  If so, what are they?**

执行了cmd.exe删除程序，并能进行读写文件操作。

**7. (4 pts) Are there any network based signatures? (URLs, packet contents. etc) If so, what are  they?**

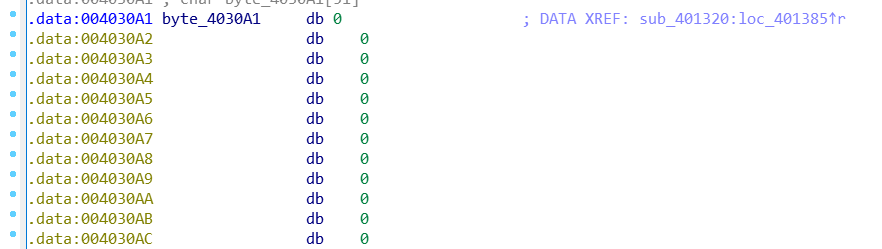
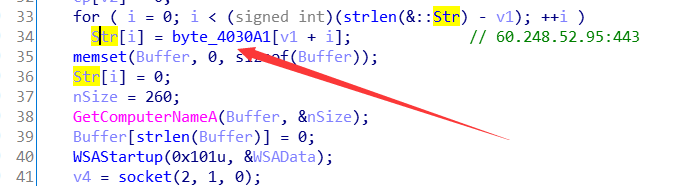
下载文件的url为http://www.ueopen.com/test.html

通信服务器为60.248.52.95，端口为443

发送的包内容为目标主机名

**8. (1 pts) Is there anything that impeded your analysis? How so? How might you overcome this?**

在用IDA静态分析时发现有些关键的字符串需要动态执行才能查看，如下图。



于是我使用Olldbg动态调试发现该字符串如下图所示，解决了问题。



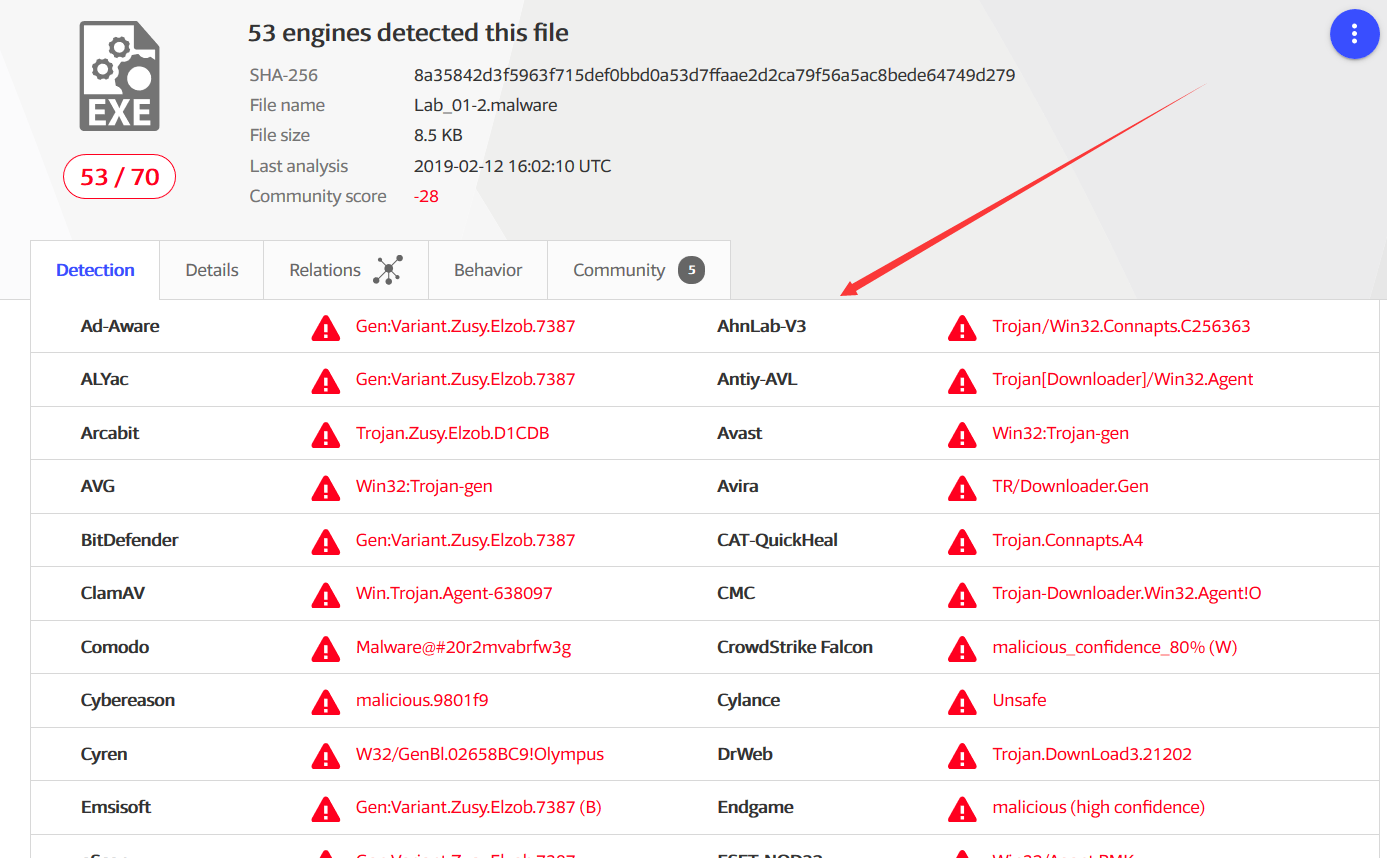
**9. (2 pts) What do you think is the purpose of this malware?**

我认为该程序的目的是获取目的主机的文件内容和权限，具体过程为从目的主机读取文件内容发送给服务器，并从服务器接收文件复制到目的主机，最后在程序执行结束时删除程序，防止留下痕迹。

**Lab\_01­2.malware**

1. **(1 pts) What is the md5sum? What of interest does VirusTotal Report?**

Md5校验和为02658bc9801f98dfdf167accf57f6a36。



**2. (6 pts) List a few imports or sets of imports and describe how the malware might use them.**

a. WriteFile，GetWindowsDirectoryA，ReadFile。该程序使用这些函数获取主机内的目录，并对主机上的文件进行读写操作。

b. InternetReadFile,HttpEndRequestA,InternetWriteFile,HttpSendRequestExA,HttpSendRequestA,InternetCloseHandle,InternetSetOptionA,InternetQueryOptionA,HttpOpenRequestA,InternetConnectA,InternetOpenA。该程序使用这些函数与服务器进行连接交互，并从服务器读取文件，在主机上写入文件。

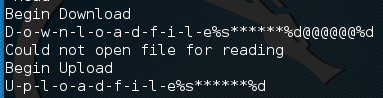
c. Sleep。该程序使用sleep函数进行暂停，等待操作。

**3. (6 pts) What are a few strings that stick out to you and why?**

a. 如下图，这些字符串说明该程序与服务器进行通信，并发送包。



b. 如下图，这些字符串说明该程序与服务器进行下载和上传文件的操作。

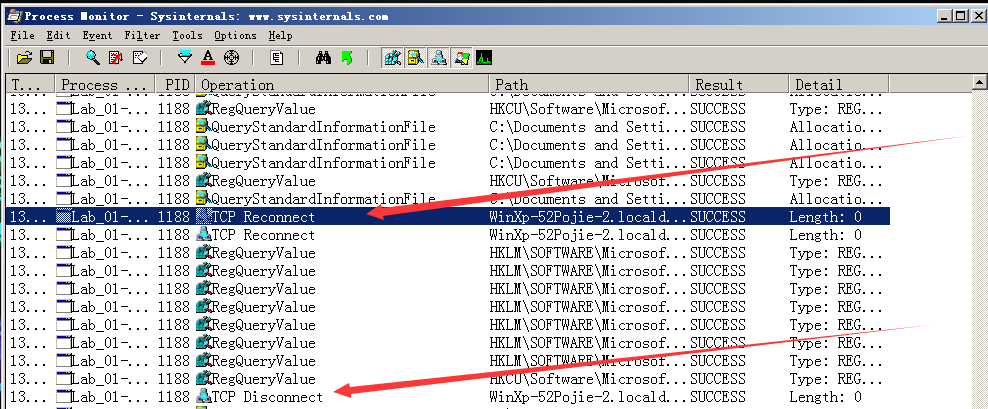


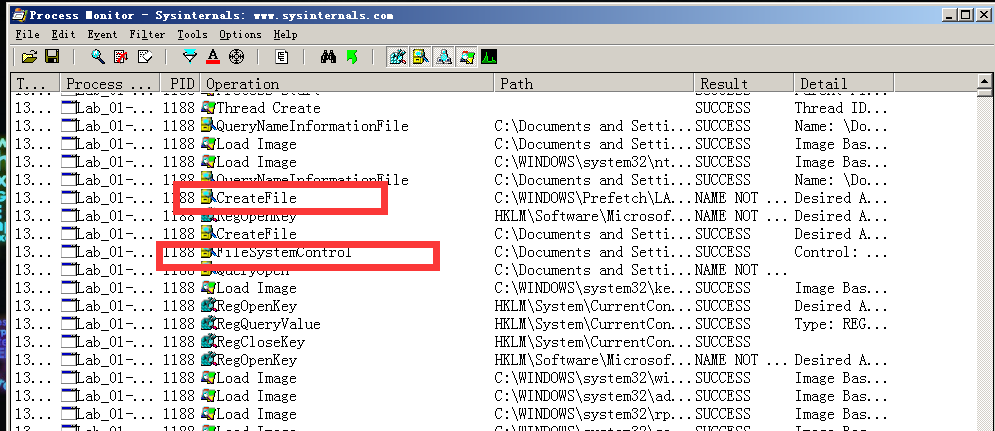
c. 如下图，这些字符串说明该程序在主机上执行cmd进行一些操作。



**4. (2 pts) What happens when you run this malware? Is it what you expected and why?**

通过process monitor监视程序，可以看到程序进行了TCP连接，文件的读写操作，和预期相同。



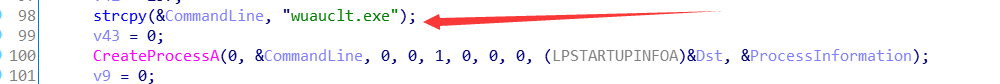


**5. (2 pts) Name a procmon filter and why you used it.**

Process monitor。因为通过过滤器的设置可以只监视特定程序的操作。

**6. (4 pts) Are there any host­based signatures? (Files, registry keys, processes or services, etc).  If so, what are they?**

执行了wuauclt.exe

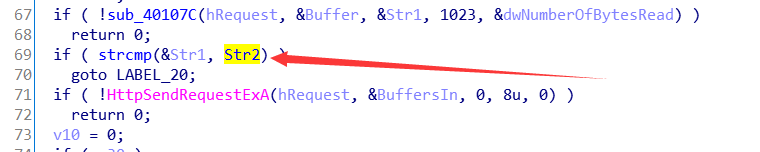
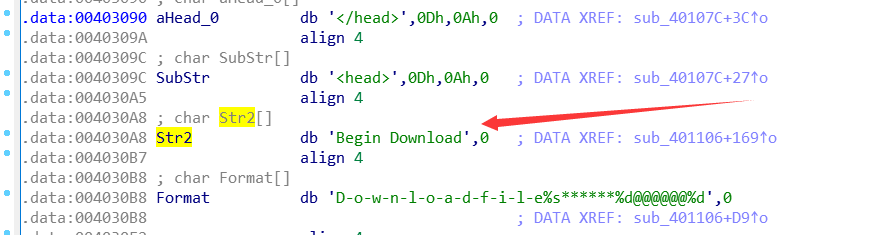


**7. (4 pts) Are there any network based signatures? (URLs, packet contents. etc) If so, what are  they?**

与69.25.50.10进行连接



由于TCP连接失败，故没有监控到有后续发包的情况。

但是通过IDA静态分析可以看到，存在“Begin Download”字样，说明当连接成功后将会进行下载文件操作。 

**8. (1 pts) Is there anything that impeded your analysis? How so? How might you overcome this?**

在启动程序时无任何反馈，不知道程序到底进行了哪些操作，只能IDA静态分析。

之后使用process monitor监视程序，直观地看到程序进行了什么操作。

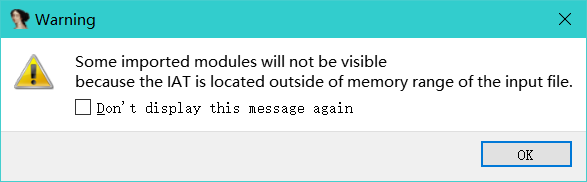
**9. (2 pts) What do you think is the purpose of this malware?**

我认为该程序的目的是在用户主机上与服务器进行连接，下载服务器上的恶意文件并将用户主机上的文件上传至服务器。

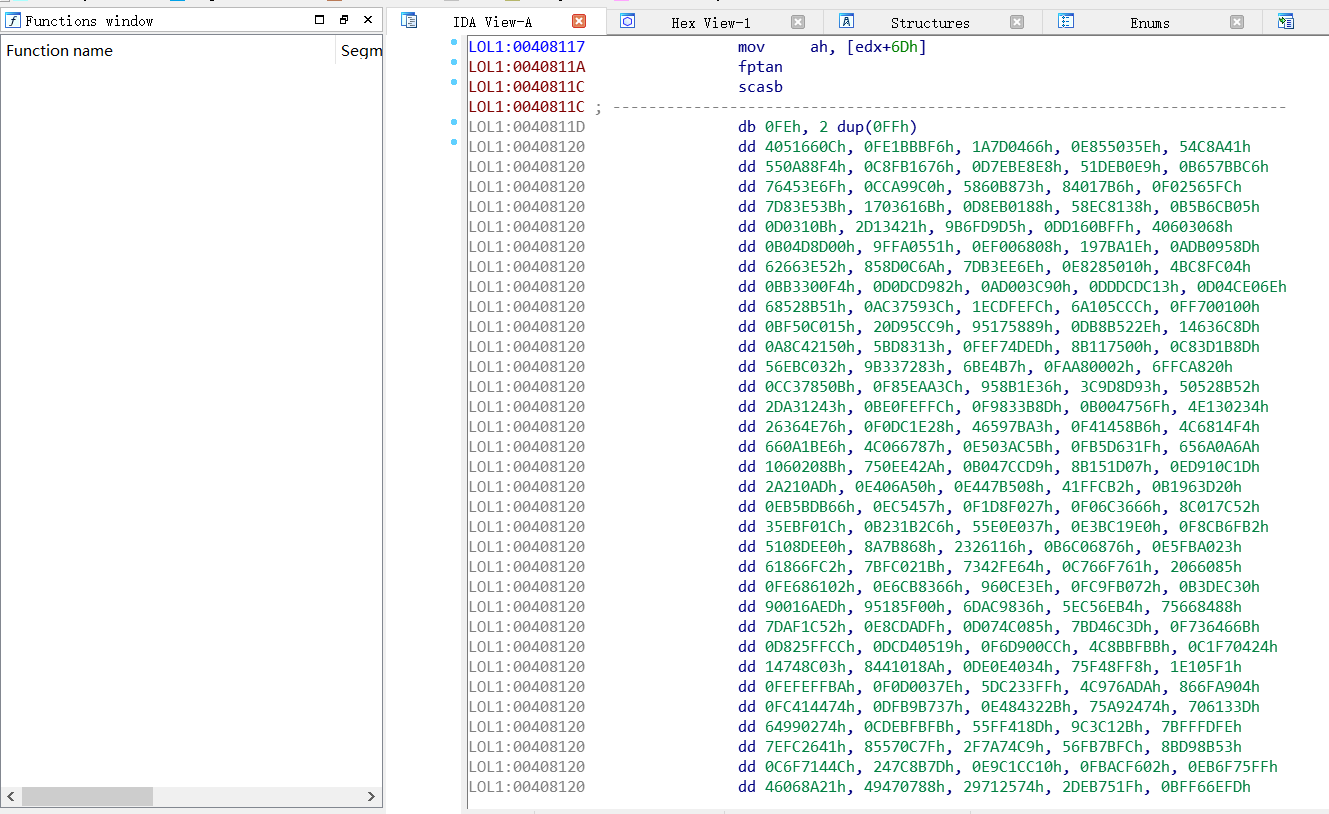
**Lab\_01­3.malware**

1. **(3 pts) Are there any indications that this malware is packed? What are they? What is it  packed with?**

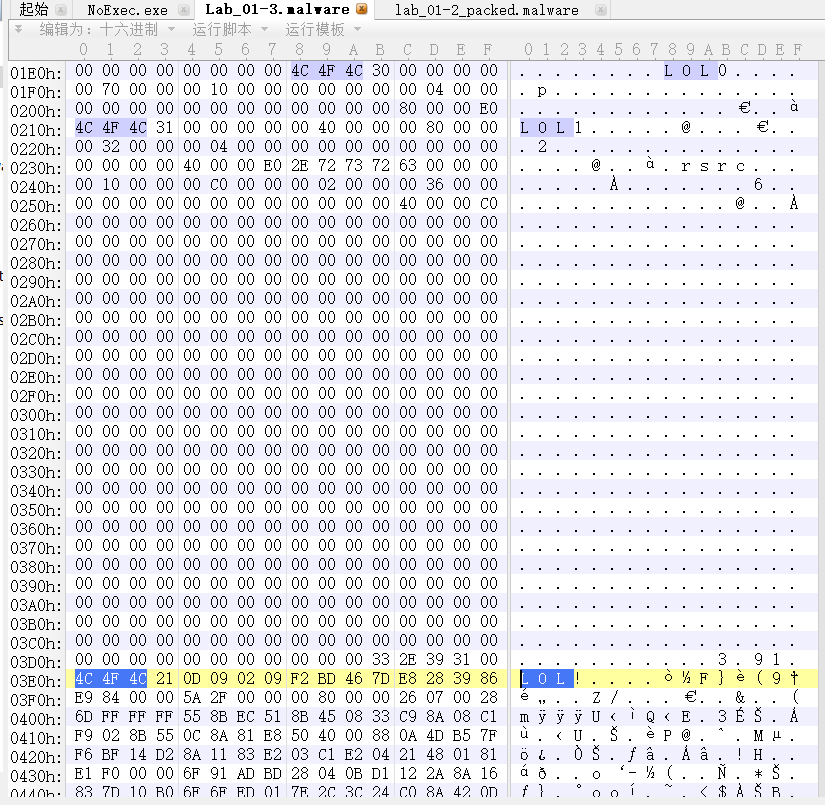
迹象1：IDA打开时有警告提示有些导入模块无法显示。



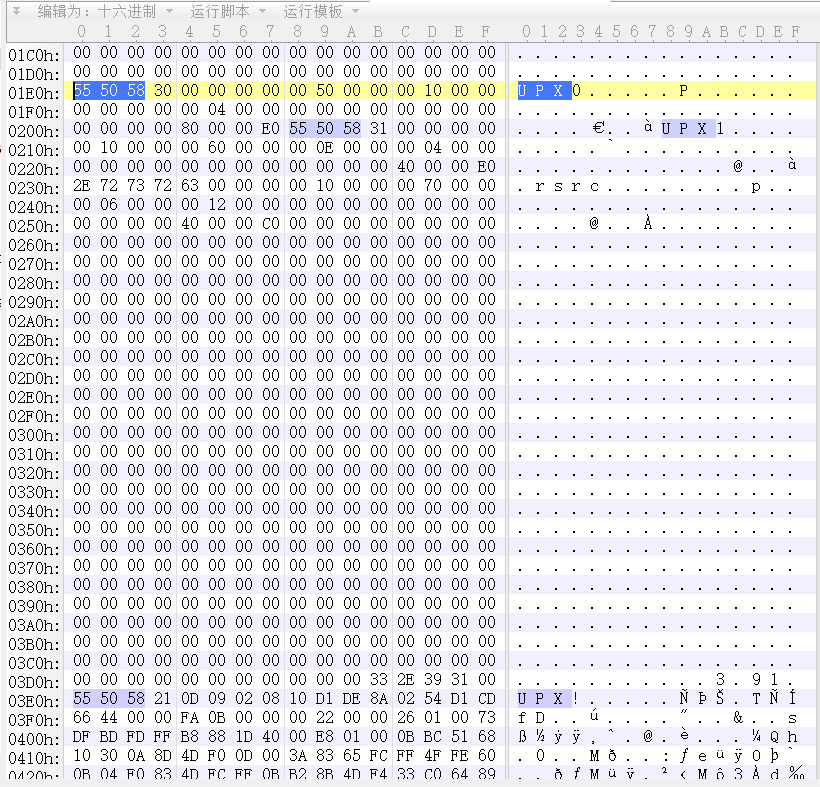
迹象2：IDA打开后左侧函数列表为空，并且右侧汇编代码处有大量位识别出的十六进制数据



迹象3：下图是该程序的二进制数据，可以看到有三个字符串“LOL”



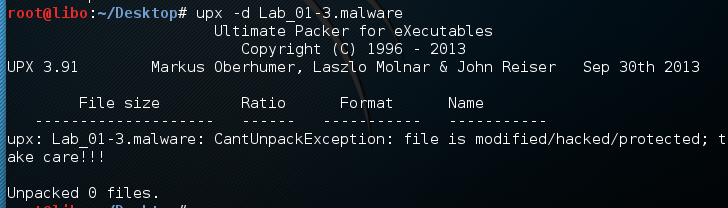
下图是经UPX加壳之后的正常程序的数据可以看到有三个字符串“UPX”



综上，可以猜测该程序经UPX加壳。

1. **(1 pts) Are you able to unpack it? Why or why not?**

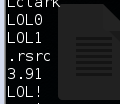
对于原始程序来说，无法直接通过upx -d命令脱壳。因为该程序被魔改了。



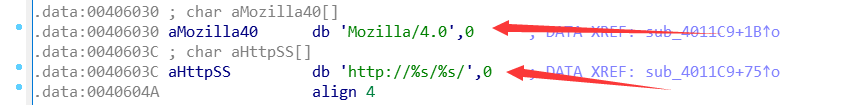
但是是能够脱壳成功的，这个会在后续问题中回答，并且后续有些回答建立在已经脱壳的前提。

1. **(3 pts) What are a few strings that stick out to you and why?**

如下图，三个LOL字符串让我联想到UPX加壳。



如下图，Mozilla/4.0字符串是useragent的一部分，说明该程序在构造http报，http://%s/%s/字符串说明该程序在构造url。

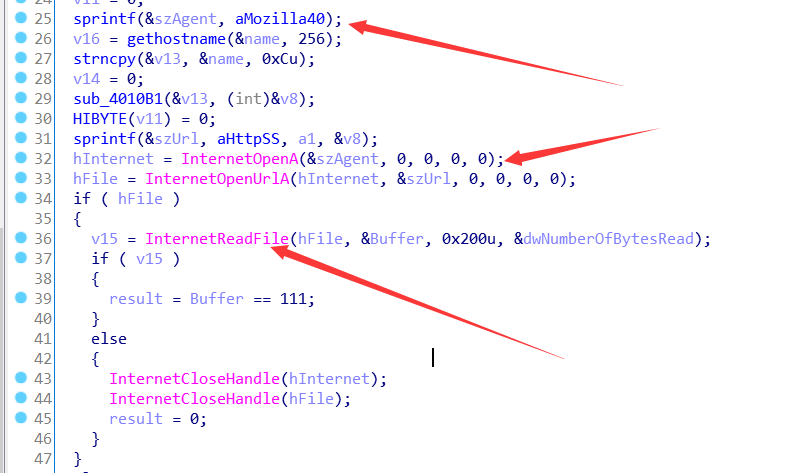


1. **(2 pts) What happens when you run this malware? Is it what you expected and why?**

通过process monitor可以看到程序在与<https://192.0.78.24>进行通信



通过IDA静态分析可以看到程序也确实进行了网络连接，读取文件的操作。

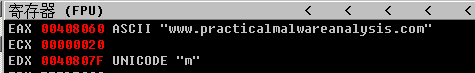


1. **(2 pts) Are there any host­based signatures? (Files, registry keys, processes or services, etc).  If so, what are they?**

用IDA静态分析时没有发现什么信息。

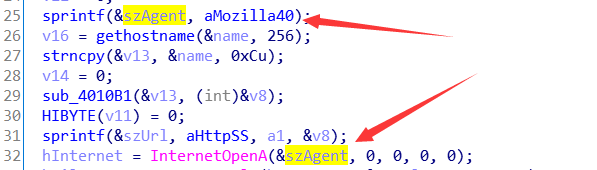
1. **(4 pts) Are there any network based signatures? (URLs, packet contents. etc) If so, what are  they?**

用Olldbg动态调试可以看到程序通信的目标是如下图的网站。



并且伪造成Mozilla访问

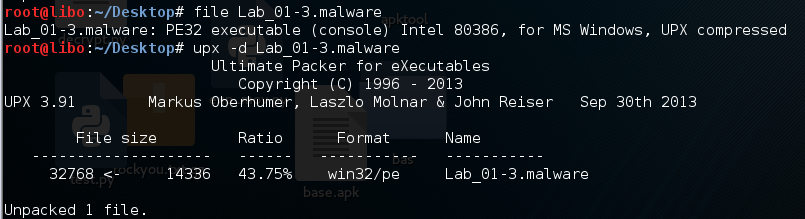




1. **(3 pts) Is there anything that impeded your analysis? How so? How might you overcome this?**
2. 在分析过程中的一个困难是该程序的upx壳被魔改了无法直接upx -d脱壳。

于是将三个字符串“LOL”改成“UPX”，再进行upx -d操作。

如下图，可以看到此时通过file命令可以判断出该程序经过upx压缩，并且upx -d命令也可以执行成功。



1. 在IDA静态分析时无法看出程序通信的目标是谁。



通过Olldbg动态调试即可解决。

1. **(2 pts) What do you think is the purpose of this malware?**

我认为该程序的目的是与网站[www.practicalmalwareanalysis.com](http://www.practicalmalwareanalysis.com)进行**不断**地通信，获取信息。

