**Lab 02 ­ Advanced Static Analysis**

**1120162015 李博**

**Lab\_02­1.malware**

**1. (10%) Main function:**

**a. What is the address of main?**

0x4011A0

**b. What does this function do?**

判断能否连接http://reversing.rocks/，若能则进入下一个函数，否则退出。

**i. What code constructs are used in this function?**

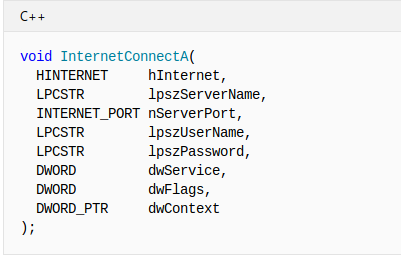
首先判断能否连接http://reversing.rocks/，如果连接成功则进入函数sub\_401130，否则异常退出。

**ii.Are there any interesting strings? If so, what are they?**

http://reversing.rocks/

**2. (15%) Looking at the subroutine a 0x00401130:**

**a.What are the arguments to InternetConnectA? What do they mean?**



hInternet是**InternetOpenA函数返回的句柄**，用于初始化程序对WinINet函数的使用，这里的v0即InternetOpenA返回的句柄；

lpszServerName代表**服务器的主机名**，这里指“reversing.rocks”；

nServerPort代表服务器上的**传输控制协议/ Internet协议（TCP / IP）端口**，这里指1234；

lpszUserName和lpszPassword代表登陆的**用户名和密码**，这里为空；

dwService代表**所用服务的类型**，这里的3指http服务；

dwFlags特定于所用服务的选项，dwContext用于标识回调中返回句柄的应用程序上下文。

**b. What does this function do?**

该函数用来连接主机名为reversing.rocks的服务器，若连接成功则进入函数sub\_401000。

**i.What code constructs are used in this function?**

连接reversing.rocks，端口号为1234，并进入函数sub\_401000。

**3. (10%) Looking at the subroutine at 0x00401000:**

**a.What code constructs are used in this function?**

首先在本机寻找符合通配符“//\*”的文件，若无结果则异常退出。否则进行http的post请求，并上传本机文件至服务器。

**b. What imported functions are called?**

FindFirstFileA，HttpOpenRequestA，HttpEndRequestA，HttpSendRequestExA，InternetWriteFile，InternetCloseHandle，FindClose

**c. What does this subroutine do?**

遍历本机内的所有文件，并上传至服务器reversing.rocks。

1. **(15%) What does this malware do?**

连接服务器reversing.rocks，遍历本机内的所有文件，并上传。

**Lab\_02­2.malware**

**1. (15%) Main function:**

**a. What imported functions are called?**

AllocConsole，FindWindowA，ShowWindow，fopen，fputs，fclose，time，ctime

**i. What do these functions do?**

AllocConsole用于打开新的控制台，并显示调试信息；

FindWindowA用于寻找名为ConsoleWindowClass的窗体；

ShowWindow用于显示窗体；

Fopen，fputs，fclose用于对文件的打开，写入和关闭。

Time用于获取当前时间，ctime用于转换time获得的秒数为标准时间的字符串。

**ii. Any interesting strings?**

“Started logging:”表示开始记录日志，说明后续操作中会不断进行写入文件。

**2. (15%) Looking at the subroutine at 0x0040135C:**

**a. What imported functions are called?**

GetAsyncKeyState

Fopen，fputc，fseek，fread，fclose

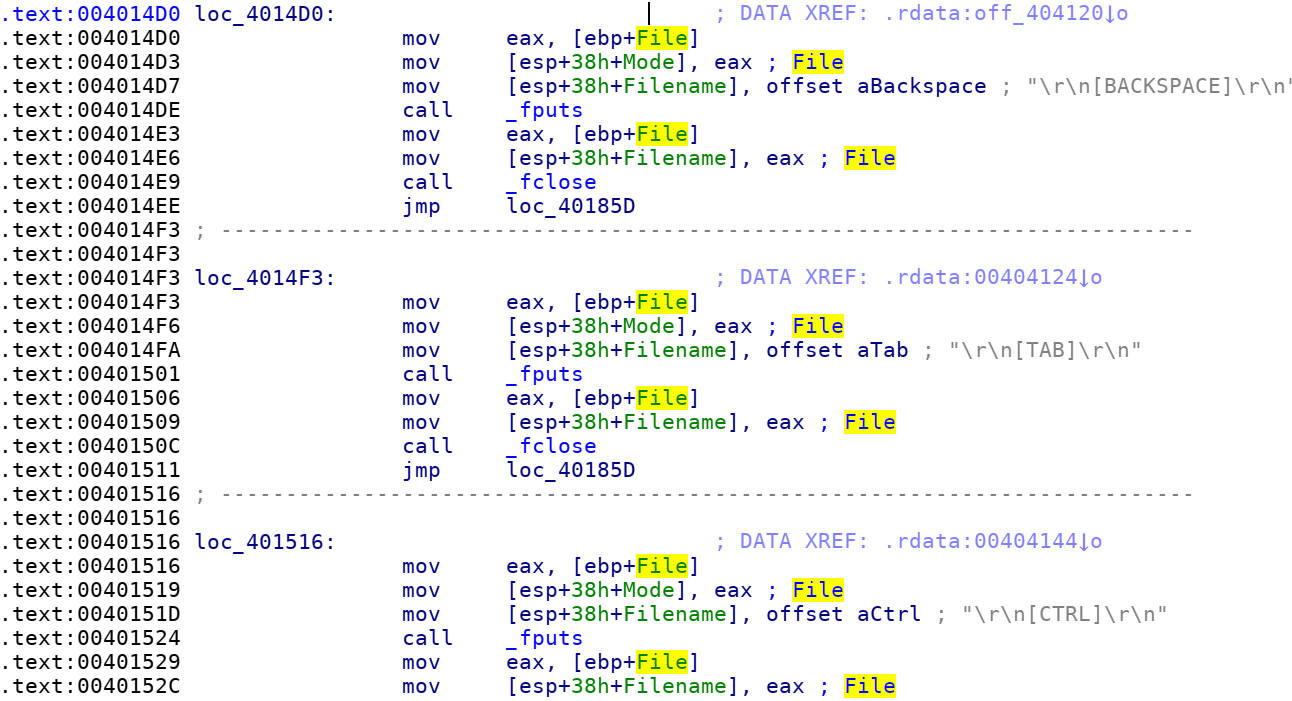
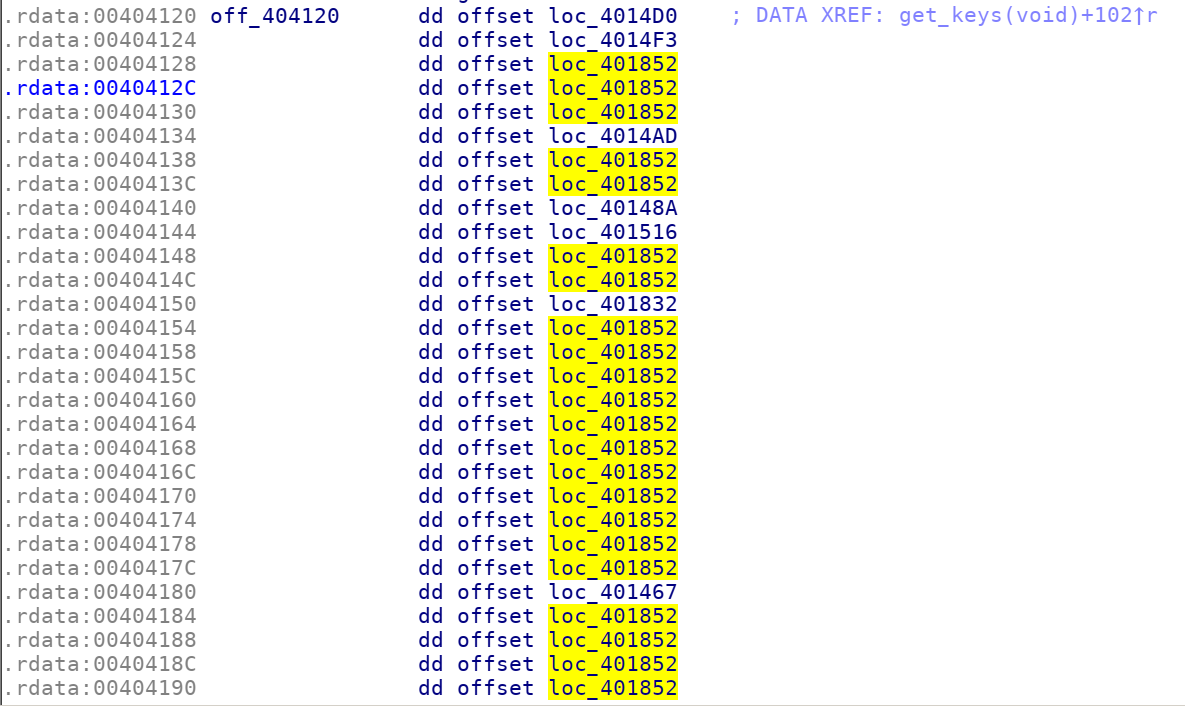
**b. What code constructs are used here?**

**Hint: Look at the ‘jmp eax’ at 0x00401465, try to guess where that jump could potentially**

**take you**

多个if分支

0x00401465处的jmp eax即根据当前按键的值跳转到相应的写入文件的操作指令。



1. **(20%) What does this malware do?**

键盘记录器，当文件大小超过100字节时，调用函数MailIt进行邮件发送。

1. **What signatures would you propose?**

GetAsyncKeyState

**i. Why are they useful signatures?**

因为它能获取键盘按键是否被按下。

**ii. Does the sample create any files? If so, what are they used for?**

有进行创建文件的操作，文件路径为\\WINDOWS\\lzwindowlz.av。

该文件用于键盘按键的使用记录。