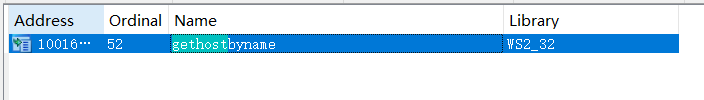
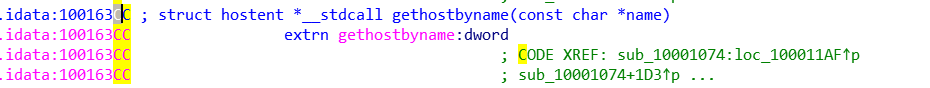
**Lab5-01 – Analysis**

**1120162015 李博**

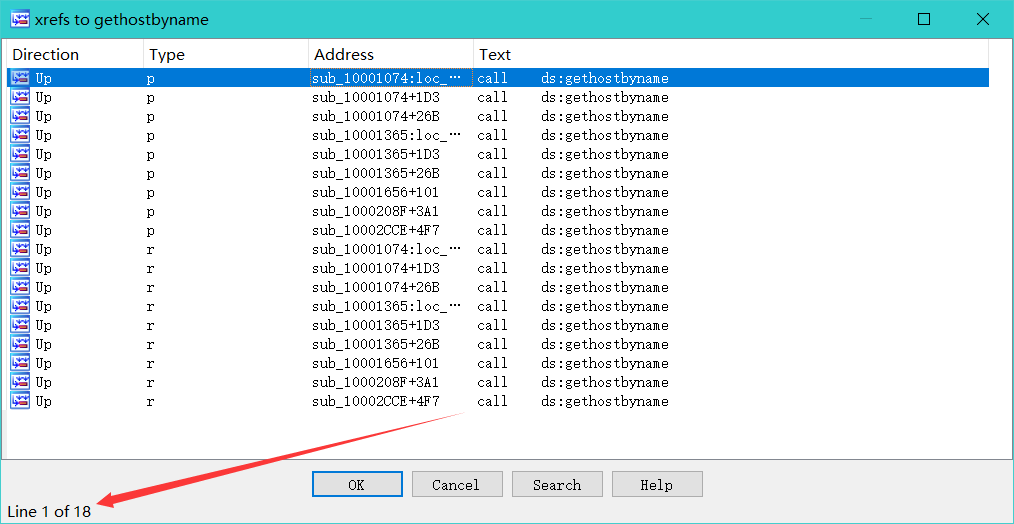
1. DLLMain的地址为0x1000D02E



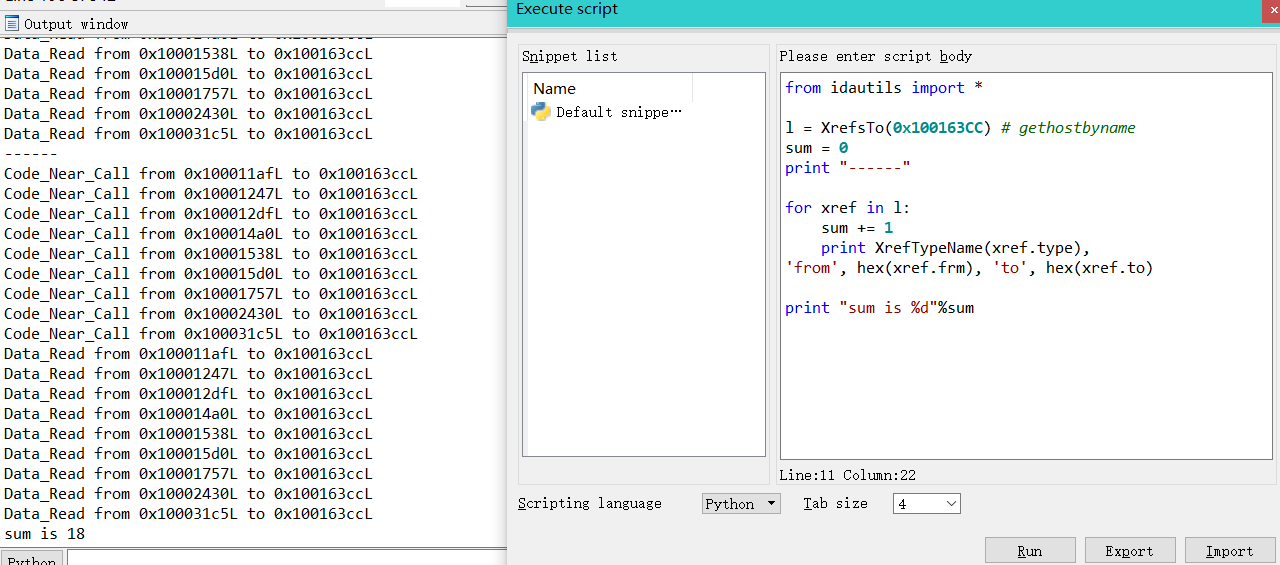


1. 18个

方法一：快捷键x



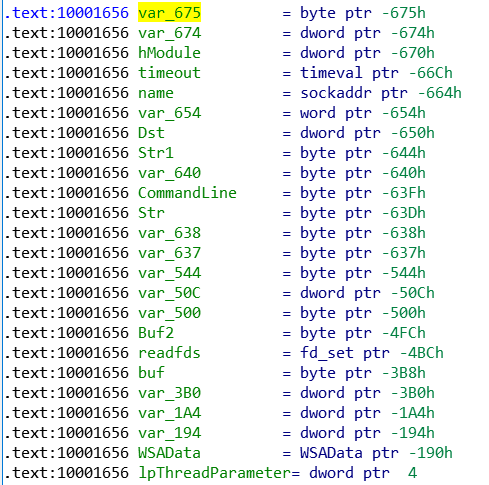
方法二：利用idapython编写脚本计数



1. pics.praticalmalwareanalysis.com



1. 24个局部变量



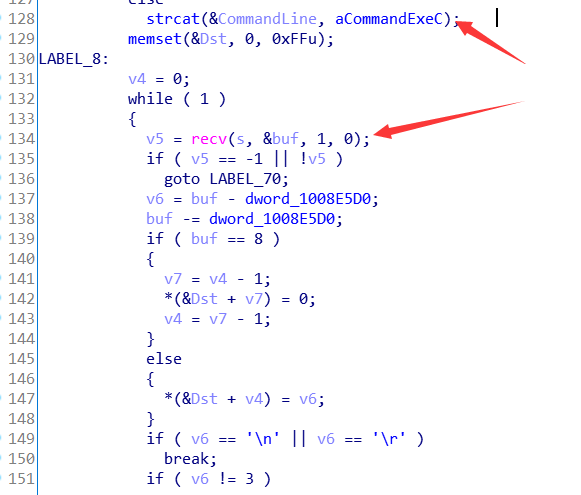
1. 1个参数

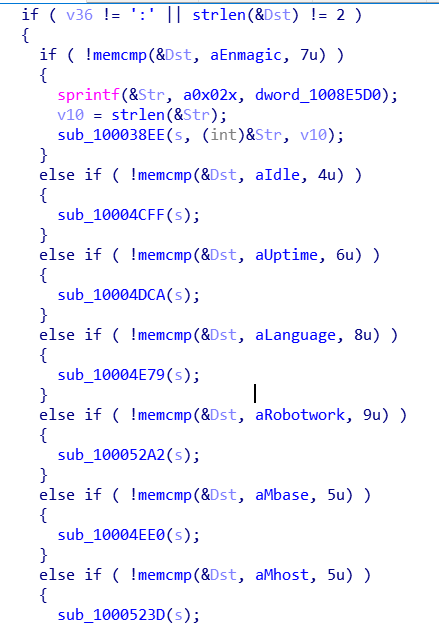




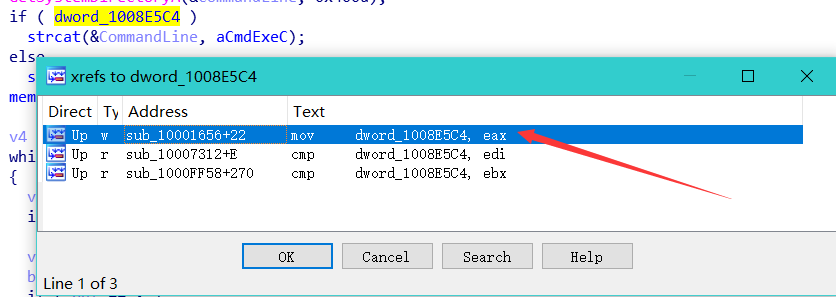


1. 调用命令行，接着一个while循环，接收远程发来的字符串，并根据接收数据的不同进入相应的处理函数。





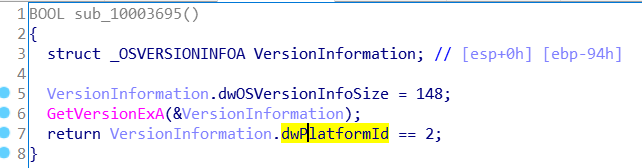
1. 通过x快捷键查看dword\_1008E5C4的交叉引用，可知dword\_1008E5C4在函数sub\_10001656+22处被赋值。



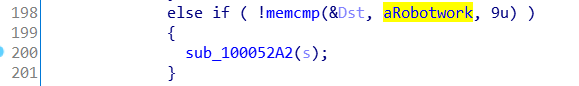
并且dword\_1008E5C4的值即函数sub\_10003695的返回值，如下图



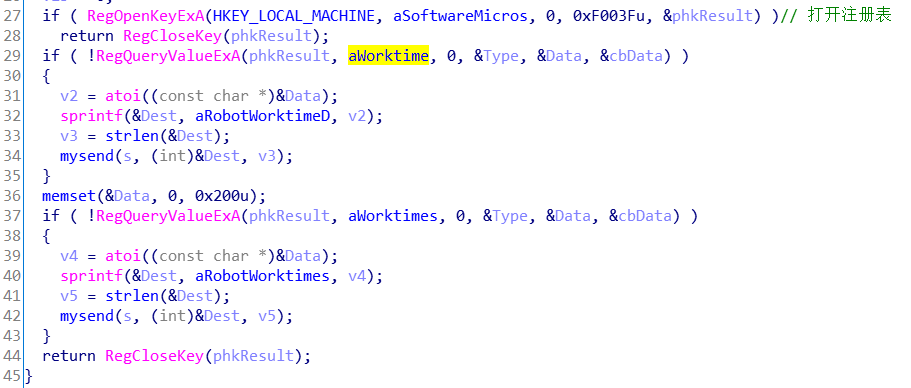
而函数sub\_10003695实际上是判断电脑的版本号是否为Microsoft Windows NT 4.0。







函数sub\_100052A2的功能就是打开电脑的注册表SOFTWARE\Microsoft\Windows\CurrentVersion，并获取字段WorkTime和WorkTimes的值，并发送给远程服务器。



1. 获取进程信息
2. API函数有memset，GetSystemDefaultLangID

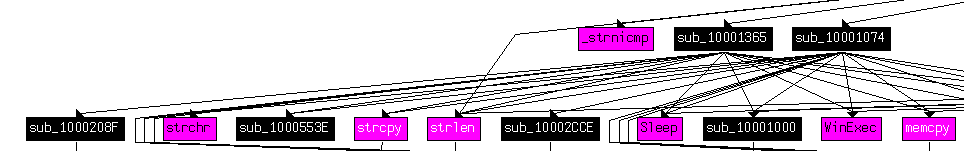
该函数用于获取系统使用的语言的id，并发送给远程服务器。



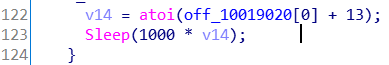
两个strlen和strncpy。

第二层有Sleep，WSAStartup，LoadLibraryA，GetProcAddress，closesocket，socket，WSAGetLastError，gethostbyname，WinExec，atoi，send等。

通过View-Graphs-User xrefs chart，设置深度为2，得到部分结果如下图。



1. Sleep 30秒



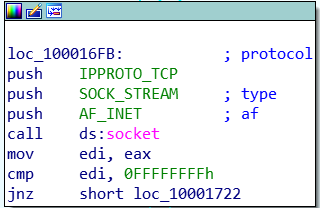
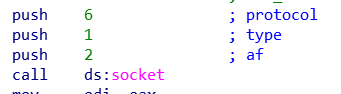


off\_10019020[0]指向的地址为0x100192AC，加上偏移13，指向的字符串为“30”，经过atoi函数得到数字30。

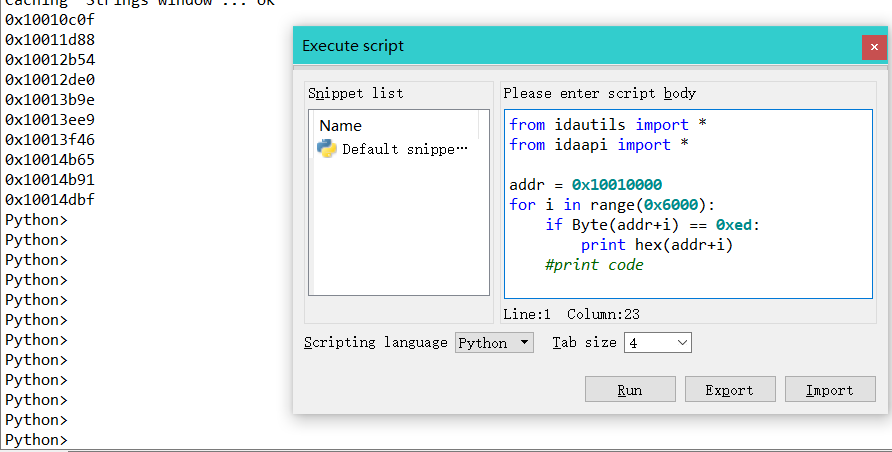
1. 2 1 6



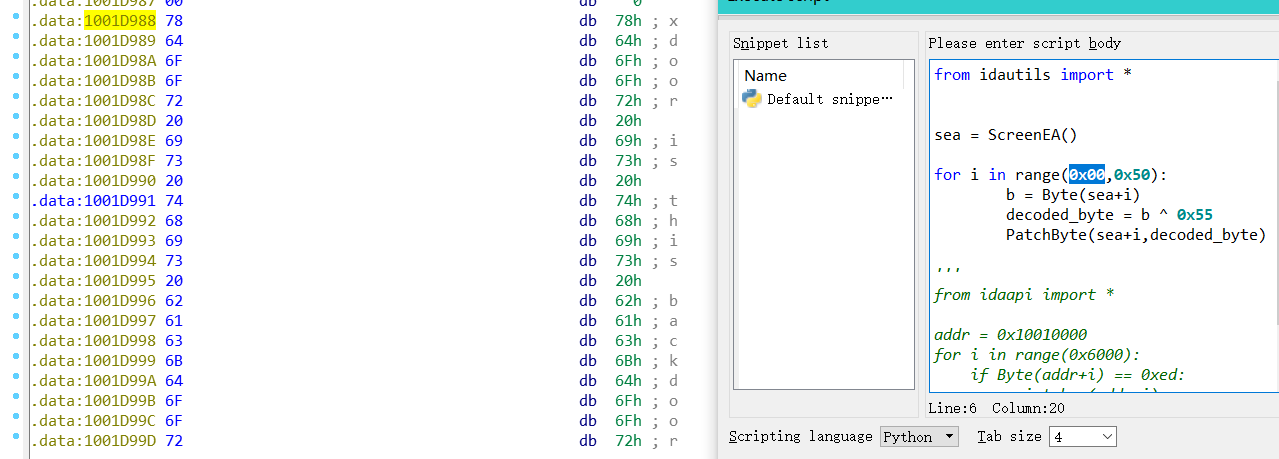
1. 查询scoket函数文档可知，第一个参数af的2代表Internet IP Protocol，第二个参数type为1代表SOCK\_STREAM，第三个参数protocol为6代表使用的协议是TCP协议。



1. 在这个恶意程序中没有找到指令in，如下图，虽然机器码有0xed，但经过校验没发现指令in。

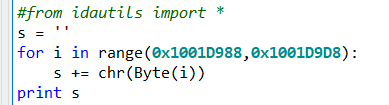


1. 地址0x1001D988处有大量可见字符，毫无意义。
2. 当运行脚本之后，0x1001D988开始的字符变成有意义的字符串



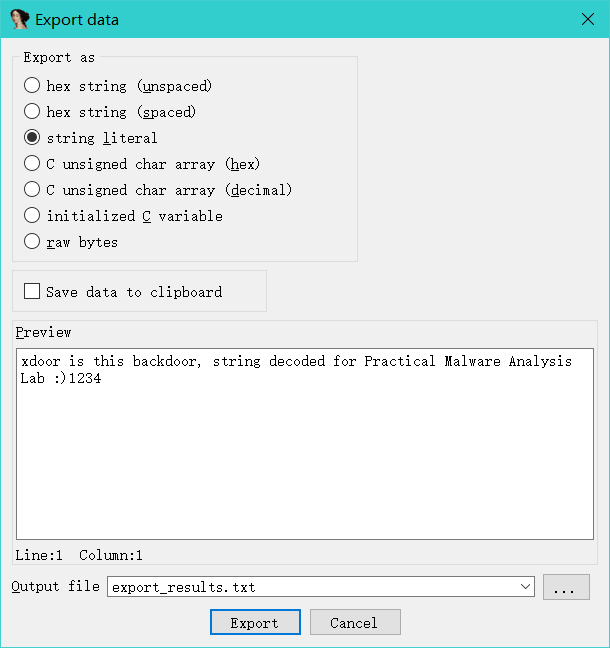
1. ‘’

方法一：idapython脚本





方法二：选中需要转换的数据，shift+E





方法一：通过Alt+F7加载py文件

方法二：shift+F2打开命令窗口直接执行代码