windows样本高级静态分析之识别汇编中C代码结构

yong夜 / 2019-10-04 09:45:01 / 浏览数 5062 安全技术 二进制安全 顶(0) 踩(0)

目标

通过分析代码结构来理解一个恶意样本的总体功能

分析流程

- 1.基础静态分析
- 2.基础动态分析
- 3.高级静态分析

实践过程

实例1

Lab06-01.exe

基础静态分析

■■■wininet.dll■kernel32.net

 \blacksquare \blacksquare \blacksquare InternetGetConnectedState

■■■■■Error 1.1: No Internet Success: Internet Connection

从导入库、导入函数、以及字符串可以看出该样本存在检测网络状态的功能

基础动态分析

C:\Users\15pb-win7\Desktop\Chapter_6L>C:\Users\15pb-win7\Desktop\Chapter_6L\Lab06-01.exe Success: Internet Connection

C: Wsers \15pb-win7\Desktop\Chapter_6L>C: Wsers \15pb-win7\Desktop\Chapter_6L\Lab06-01.exe Error 1.1: No Internet

运行样本后,通过联网和断网两种情景样本打印出不同输出,基本可以确定存在网络状态检测功能

高级静态分析

通过一个if-else语句,根据不同网络状态返回值来打印不同的字符串,并且根据基础动态分析的反馈可以判断sub_40105F函数为printf函数

```
.cexc:00401000
.text:00401000 sub 401000
                                                         ; CODE XREF: _main+41p
                                proc near
.text:00401000
                                = dword ptr -4
.text:00401000 var 4
.text:00401000
.text:00401000
                                bush
                                         ebo
.text:00401001
                                mov
                                        ebp, esp
.text:00401003
                                push
                                        ecx
.text:00401004
                                push
                                         0
                                                          ; dwReserved
.text:00401006
                                         ß
                                push
                                                          ; lpdwFlags
.text:00401008
                                        ds:InternetGetConnectedState
                                call
                                         [ebp+var_4], eax
.text:0040100E
                                mov
                                         Cebo+uar 41
.text:00401011
                                e m
.text:00401015
                                įΖ
                                        short loc 40102B
                                                                   "Success: Internet Connection\n"
.text:00401017
                                push
                                        offset aSuccessInterne
.text:0040101C
                                call
                                        sub 40105F
                                                                   if语句
.text:00401021
                                add
                                        esp, 4
.text:00401024
                                mov
                                        eax, 1
.text:00401029
                                         short loc_40103A
                                jmp
.text:0040102B
.text:0040102B
                                                          ; CODE XEF: sub_401000+15ij
.text:00401028 loc_401028:
                                         offset aError1_1NoInte ; "Error 1.1: No Internet\n"
.text:0040102B
                                push
.text:00401030
               else语句
                                call
                                        sub_40105F
.text:00401035
                                add
                                         esp, 4
.text:00401038
                                xor
                                         eax, eax
.text:0040103A
.text:0040103A loc_40103A:
                                                          ; CODE XREF: sub_401000+291j
.text:0040103A
                                mov
                                         esp, ebp
.text:0040103C
                                pop
                                        ebp
.text:0040103D
                                retn
.text:0040103D sub 401000
                                endp
text:00L0103D
```

实例2

基础静态分析

导入函数

InternetOpenUrlA
InternetCloseHandle
InternetReadFile
InternetGetConnectedState
InternetOpenA

Success: Parsed command is %c

字符串

http://www.practicalmalwareanalysis.com/cc.htm Error 1.1: No Internet Success: Internet Connection Error 2.3: Fail to get command Error 2.2: Fail to ReadFile Error 2.1: Fail to OpenUrl Internet Explorer 7.5/pma

从导入函数和字符串可以看出,这个样本应该对网页发起请求,并且可能存在解析网页来获取命令的操作

基础动态分析

```
C: Wsers \15pb-win7\Desktop\Chapter_6L>C: Wsers \15pb-win7\Desktop\Chapter_6L\Lab06-02.exe
Success: Internet Connection
Error 2.1: Fail to OpenUrl
C:\Wsers\15pb-win7\Desktop\Chapter_6L>_
```

根据返回的信息,是访问url失败,手动在浏览器访问该网页缺失已经实效

高级静态分析

```
3
3
                   push
                           ebp
1
                   mov
                           ebp, esp
3
                   sub
                           esp, 8
                           sub 401000
5
                   call
3
                   mov
                            [ebp+var_4], eax
                            [ebp+var 4], 0
                   cmp
2
                           short loc_401148
                   jnz
4
                   ¥or
                           eax, eax
5
                   jmp
                           short loc 40117B
3
                            l if语句
 loc_401148:
                                             ; CODE XREF: _main+12fj
3
3
                           sub 401040
                   call
)
                   mov
                           [ebp+var_8], al
3
                           eax, [ebp+var_8]
                   MOVSX
4
                   test
                           eax. eax
5
                           short loc 40115C
                   jnz
3
                   xor
                           eax, eax
                   jmp
                           short loc_40117B
                         ·if语句内的第一个idi语句EF: _main+26fj
  loc 40115C:
)
                   MOVSX
                           ecx, [ebp+var_8]
9
                   push
                           ecx
1
                           offset aSuccessParsedC ; "Success: Parsed command is %c\
                   push
5
                           sub 40117F
                   call
3
                   add
                           esp, 8
Ξ
                   push
                                             ; dwMilliseconds
                            0EA60h
3
                   call
                           ds:Sleep
7
                   xor
                           eax, eax
3
                                             ; CODE XREF: _main+16îj
3 loc_40117B:
3
                                             ; _main+2Aîj
3
                           esp, ebp
                   mov
)
                   pop
                           ebp
                   retn
  _main
                   endp
```

跟进main函数分析代码得到只有跟进上面的两个if语句内部,即满足这两个if语句的成立条件才可以打印出'Success: Parsed command is %c',而如果不满足条件就会退出,接着我们跟进sub_401000函数,分析如果满足第一个if语句的跳转条件

```
.text:00401000
                                                          ; CODE XREF: _main+6_p
.text:00401000 sub_401000
                                proc near
.text:00401000
.text:00401000 var_4
                                = dword ptr -4
.text:00401000
.text:00401000
                                push
                                        ebp
.text:00401001
                                mov
                                        ebp, esp
.text:00401003
                                        ecx
                                push
.text:00401004
                                                          ; dwReserved
                                push
                                         0
.text:00401006
                                push
                                                           1pdwF1ags
.text:00401008
                                call
                                        ds:InternetGetConnectedState
                                         <u>[ebo+var 4]. eax</u>
.text:0040100E
                                MOV
                                         [ebp+var 4], 0
.text:00401011
                                cmp
.text:00401015
                                        short loc 40102B
                                iΖ
.text:00401017
                                        offset aSuccessInterne ; "Success: Internet Connect
                                push
.text:0040101C
                                call
                                        sub 40117F
.text:00401021
                                add
                                        esp, 4
                                                      if语句块
.text:00401024
                                mov
                                        eax, 1
.text:00401029
                                        short loc 40103A
                                jmp
.text:0040102B
.text:0040102B
                            if-else语句中的else语句块 ; CODE XREF: sub_401000+15fj
.text:0040102B loc_40102B:
                                        offset aError1_1NoInte; "Error 1.1: No Internet\n'
.text:0040102B
                                push
.text:00401030
                                call
                                        sub_40117F
.text:00401035
                                add
                                        esp, 4
.text:00401038
                                xor
                                        eax, eax
.text:0040103A
                                                          ; CODE XREF: sub 401000+291j
.text:0040103A loc 40103A:
.text:0040103A
                                         esp, ebp
                                mov
.text:0040103C
                                        ebp
                                pop
.text:0040103D
                                retn
.text:0040103D sub 401000
                                endp
.text:0040103D
```

直接跟进sub_401000函数,和实例1的功能一样,需要联网才可以返回为1,即满足一个if成立条件

```
LEXE.00401040
                               pusii
text:00401041
                               mov
                                       ebp, esp
                                       esp, 210h
text:00401043
                               sub
text:00401049
                               push
                                       A
                                                         dwFlags
text:0040104B
                               push
                                       A
                                                          1pszProxyBypass
text:0040104D
                                       0
                               push
                                                          1pszProxy
text:0040104F
                               push
                                       0
                                                          dwAccessType
text:00401051
                               push
                                       offset szAgent
                                                          "Internet Explorer 7.5/pma"
text:00401056
                               call
text:0040105C
                                       [ebp+hInternet], eax
                               mov
text:0040105F
                               push
                                                        ; dwContext
text:00401061
                                       0
                                                          dwFlags
                               push
text:00401063
                                                          dwHeadersLength
                                       ø
                               push
text:00401065
                                       A
                                                          1pszHeaders
                               bush
                                                         "http://www.practicalmalwareanalysis.c
text:00401067
                                       offset szUrl
                               push
                                       eax, [ebp+hInternet]
text:0040106C
                               mov
                                                        ; hInternet
text:0040106F
                               push
                                       eax
text:00401070
                                       ds:InternetOpenUrlA
                               call
                                       <u>[ebo+hFile].</u>
                                                    eax
text:00401076
                               mov
text:00401079
                               cmp
                                       [ebp+hFile], 0
text:0040107D
                               jnz
                                       short loc 40109D
                               push
text:0040107F
                                       offset aError2_1FailTo ; "Error 2.1: Fail to OpenUrl\n"
text:00401084
                               call
                                       sub_40117F
text:00401089
                               add
                                       esp, 4
text:0040108C
                               mov
                                       ecx, [ebp+hInternet]
text:0040108F
                               push
                                                        ; hInternet
                                       ds:InternetCloseHandle
text:00401090
                               call
text:00401096
                               xor
text:00401098
                               jmp
                                       1oc_40112C
text:0040109D
text:0040109D
                                 个if语句成立后执行的通向赎F: sub_401040+3Dfj
text:0040109D loc 40109D:
                               1ea
                                       edx, [ebp+dwNumberOfBytesRead]
text:0040109D
                                                        ; 1pdwNumberOfBytesRead
text:004010A0
                               push
                                       edx
                                                          dwNumberOfBytesToRead
text:004010A1
                                       200h
                               push
text:004010A6
                                       eax, [ebp+Buffer]
                               lea.
                                                          1pBuffer
text:004010AC
                               push
                                       eax
text:004010AD
                                       ecx, [ebp+hFile]
                               mov
                               push
text:004010B0
                                       ecx
                                                         hFile
text:004010B1
                               call
                                       ds:InternetReadFile
text:004010B7
                               mou
                                       Tehn+uar 41
                                                    eav
                                       [ebp+var_4], 0
text:004010BA
                               cmp
text:004010BE
                                       short loc_4010E5
                               jnz
text:004010C0
                               push
                                       offset aError2_2FailTo ; "Error 2.2: Fail to ReadFile\n'
text:004010C5
                                       sub_40117F
                               call
text:004010CA
                               add
                                       esp, 4
text:004010CD
                               mov
                                       edx, [ebp+hInternet]
                                                        ; hInternet
text:004010D0
                               push
                                       edx
                                       ds:InternetCloseHandle
text:004010D1
                               call
text:004010D7
                                       eax, [ebp+hFile]
                               mov
text:004010DA
                               push
                                                        ; hInternet
                                       eax
text:004010DB
                                       ds:InternetCloseHandle
                               call
text:004010E1
                                       al, al
                               xor
text:004010E3
                                       short loc 40112C
                               jmp
text:004010E5
text:004010E5
                                -个if语句内部的第一个obt语包成实的语句块fj
text:004010E5 loc 4010E5:
                                       ecx, [ebp+Buffer]
text:004010E5
                               movsx
text:004010EC
                               cmp
                                       ecx, acn
text:004010EF
                               inz
                                       short loc 40111D
text:004010F1
                               movsx
                                       edx, [ebp+var_20F]
text:004010F8
                               cmp
                                       edx, 21h
text:004010FB
                               jnz
                                       short loc_40111D
text:004010FD
                               movsx
                                       eax, [ebp+var_20E]
text:00401104
                                       eax, 2Dh
                               cmp
                                       short loc_40111D
text:00401107
text:00401109
                               movsx
                                       ecx, [ebp+var_20D]
text:00401110
                                       ecx, 2Dh
                               cmp
text:00401113
                                       short loc_40111D
                               inz
text:00401115
                                       al, [ebp+var 20C]
                               mov
text:0040111B
                               imp
                                       short loc_40112C
text:0040111D
text:0040111D
text:0048111D loc_48111D: 第二层嵌套的if语句不成立跳破的語句ub 481040+AFfj
                                                        sub 401040+BBfj ..
text:0040111D
                                       offset aError2_3FailTo ; "Error 2.3: Fail to get command
text:0040111D
                               push
                                       sub_40117F
text:00401122
                               call
text:00401127
                               add
                                       esp, 4
text:0040112A
                               xor
                                       al, al
text:0040112C
                                                        ; CODE XREF: sub_401040+581j
text:0040112C loc_40112C:
text:0040112C
                                                          sub_401040+A31j
text:0040112C
                               mov
                                       esp, ebp
text:0040112E
                               pop
                                       ebp
text:0040112F
                               retn
text:0040112F sub_401040
```

数组修复

```
BOOLAPI InternetReadFile(
HINTERNET hFile,
LPVOID lpBuffer,
DWORD dwNumberOfBytesToRead,
LPDWORD lpdwNumberOfBytesRead
);
```

Parameters

hFile

Handle returned from a previous call to <u>InternetOpenUrl</u>, <u>FtpOpenFile</u>, or <u>HttpOpenRequest</u>.

1pBuffer

Pointer to a buffer that receives the data.

根据MSDN上的函数介绍,我们知道 InternetReadFile函数是向lpBuffer这个数组内写入数据的,大小有dwNumberOfBytesToRead决定在分析最后一个条件判断时,ida并没有识别出这个函数的数组长度,所以后面三个比较都是用变量var_20F等来表示的。

```
-00000210 ; D/A/*
                      : change type (data/ascii/array)
-00000210 ; N
                      : rename
                                                                                     X
                                       Convert to array
-00000210 ; U
                       : undefine
-00000210 ; Use data definition
                                                                                             arguments.
-00000210 ; Two special fields "
                                                                                             registers.
                                        Start offset
                                                     : 0x0
-00000210 ; Frame size: 210; Savi
                                        End offset
                                                     : 0x1
-00000210 ;
-0000021<mark>0</mark>
                                        Array element size
-00000021<mark>0 Buffer</mark>
-0000020F var_20F
                              db ?
                                        Maximal possible size:
                              db?
                                        Current array size
-0000020E var_20E
                              db ?
                                        Suggested array size :
-0000020D var 20D
                              Œυ
                              db
-0000020<mark>C var_20C</mark>
                                 ?
                                                              512
                                                                          (in elements)
-0000026B
                              db
                                 ?
                                        Array size
-0000020A
                              db
                                 ?
                                                              512
                                        \underline{\mathbf{I}}tems on a line
                                                                          (O-max)
                                 ?
-00000209
                              db
-00000208
                              db
                                 ?
                                                              -1
                                                                          (-1-none, 0-auto)
                                        Element print width
-00000207
                              db
                                 ?
                              db?
-00000206
                                         Options
                                                                   Indexes
-00000205
                              db ?

▼ Use "dup" construct

                                                                   Decimal
-000000204
                              db ?
-00000203
                              db ?
                                         Signed elements
                                                                   Hexadecimal
- 000000202
                              db
                                 ?
                                         Display indexes
                                                                   Octal
                                 ?
-000000201
                              db
                                         V Create as array
                                                                   Binary
-00000200
                              db
                                 ?
-000001FF
                              db
                                 ?
-000001FE
                              db
                                 ?
                                                   OK
                                                                          Help
                                                             Cancel
                                 ?
-000001FD
                              db
-000001FC
                              db
                                ?
                                     underined
-000001FB
                              db
                                    ; undefined
-000001FA
                              db ? : undefined
-000001F9
                              db ? ; undefined
-000001F8
                              db ? : undefined
手动修复数组大小为512字节
 - 000000270
                               db 512 dup(?)
 -00000210 <mark>Buff</mark>er
 -000000010 hFile
                               dd ?
                                                            ; offset
 -00000000C hInternet
                               dd ?
                                                            ; offset
 -00000008 dwNumberOfBytesRead dd ?
                               dd ?
 -000000004 var 4
 +00000000
                               db 4 dup(?)
             s
                               db 4 dup(?)
 +00000004
+000000008
  char Buffer[512]; <mark>/</mark>/ [sp+0h] [bp-210h]@3
  HINTERNET hFile; // [sp+200h] [bp-10h]@1
  HINTERNET hInternet; // [sp+204h] [bp-Ch]@1
  DWORD dwNumberOfBytesRead; // [sp+208h] [bp-8h]@3
  int v5; // [sp+20Ch] [bp-4h]@3
  hInternet = InternetOpenA(szAgent, 0, 0, 0, 0);
  hFile = InternetOpenUrlA(hInternet, szUrl, 0, 0, 0, 0);
  if ( hFile )
  {
    v5 = InternetReadFile(hFile, Buffer, 0x200u, &dwNumberOfBytesRead);
    if ( U5 )
    {
       if ( Buffer[0] != 60 || Buffer[1] != 33 || Buffer[2] != 45 || Buffer[3] != 45 )
         sub_40117F(aError2_3FailTo);
         result = 0;
       }
       else
```

点击收藏 | 0 关注 | 1

上一篇:基于qemu和unicorn的Fu... 下一篇:windows中常见后门持久化方法总结

- 1. 0条回复
 - 动动手指,沙发就是你的了!

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS <u>关于社区</u> <u>友情链接</u> <u>社区小黑板</u>