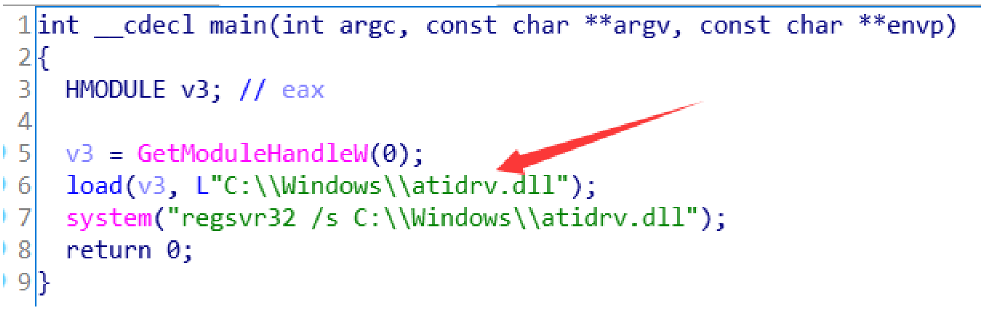
Lab_03 – analysis

1120162015 李博

Lab_03-1

1. (1 pts) Did you find any interesting resources? If so, how did you extract it?

用 ida 打开看到有 **C:\\Windows\\atidrv.dll** 字样，如下图。

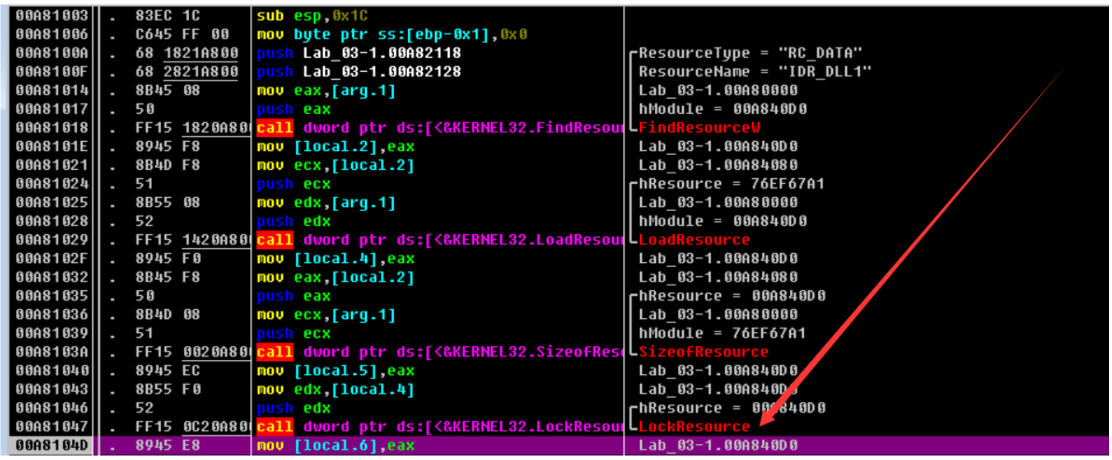


```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  HMODULE v3; // eax

  v3 = GetModuleHandleW(0);
  load(v3, L"C:\\Windows\\atidrv.dll");
  system("regsvr32 /s C:\\Windows\\atidrv.dll");
  return 0;
}
```

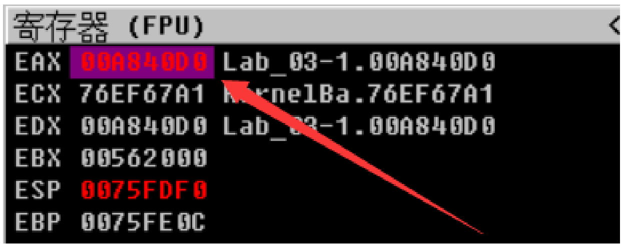
GetModuleHandleW 函数的参数为 **0** 说明是获取进程本身的句柄。

进行动态调试，如下图



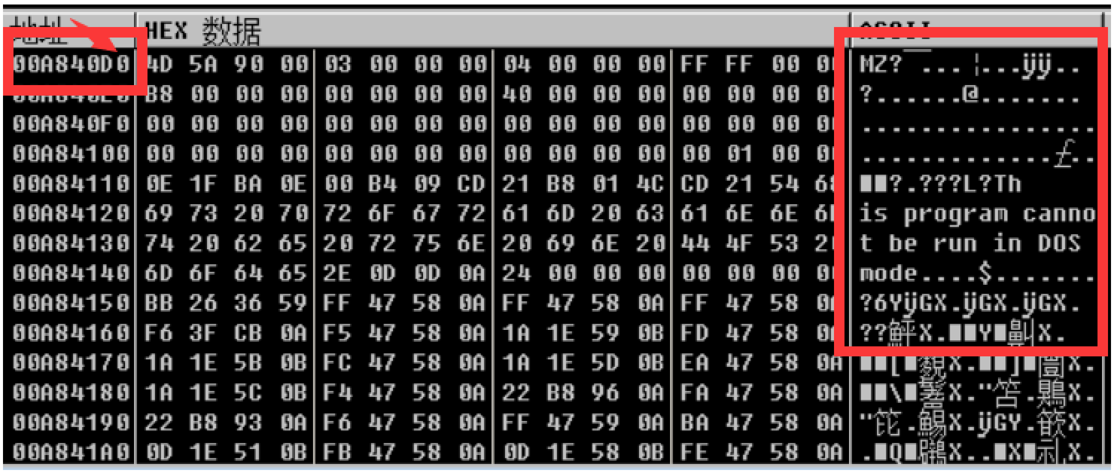
```
00A81003  .  83EC 1C          sub esp,0x1C
00A81006  .  C645 FF 00       mov byte ptr ss:[ebp-0x1],0x0
00A8100A  .  68 1821A800      push Lab_03-1.00A82118                     ┌ResourceType = "RC_DATA"
00A8100F  .  68 2821A800      push Lab_03-1.00A82128                     │ResourceName = "IDR_DLL1"
00A81014  .  8B45 08          mov eax,[arg.1]                            │Lab_03-1.00A80000
00A81017  .  50               push eax                                   │hModule = 00A840D0
00A81018  .  FF15 1820A80(    call dword ptr ds:[<&KERNEL32.FindResou    └FindResourceW
00A8101E  .  8945 F8          mov [local.2],eax                           Lab_03-1.00A840D0
00A81021  .  8B4D F8          mov ecx,[local.2]                           Lab_03-1.00A84080
00A81024  .  51               push ecx                                   ┌hResource = 76EF67A1
00A81025  .  8B55 08          mov edx,[arg.1]                            │Lab_03-1.00A80000
00A81028  .  52               push edx                                   │hModule = 00A840D0
00A81029  .  FF15 1420A80(    call dword ptr ds:[<&KERNEL32.LoadResou    └LoadResource
00A8102F  .  8945 F0          mov [local.4],eax                           Lab_03-1.00A840D0
00A81032  .  8B45 F8          mov eax,[local.2]                           Lab_03-1.00A84080
00A81035  .  50               push eax                                   ┌hResource = 00A840D0
00A81036  .  8B4D 08          mov ecx,[arg.1]                            │Lab_03-1.00A80000
00A81039  .  51               push ecx                                   │hModule = 76EF67A1
00A8103A  .  FF15 0020A80(    call dword ptr ds:[<&KERNEL32.SizeofRes    └SizeofResource
00A81040  .  8945 EC          mov [local.5],eax                           Lab_03-1.00A840D0
00A81043  .  8B55 F0          mov edx,[local.4]                           Lab_03-1.00A840D0
00A81046  .  52               push edx                                   ┌hResource = 00A840D0
00A81047  .  FF15 0C20A80(    call dword ptr ds:[<&KERNEL32.LockResou    └LockResource
00A8104D  .  8945 E8          mov [local.6],eax                           Lab_03-1.00A840D0
```

当 load_resource 结束之后，eax 指向的便是资源所在首地址，如下图。



```
寄存器 (FPU)
EAX 00A840D0 Lab_03-1.00A840D0
ECX 76EF67A1 KernelBa.76EF67A1
EDX 00A840D0 Lab_03-1.00A840D0
EBX 00562000
ESP 0075FDF0
EBP 0075FE0C
```

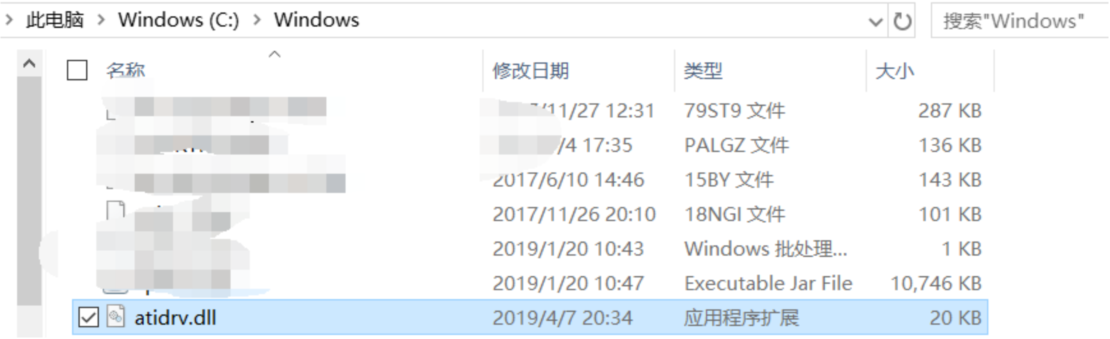
右键数据窗口中跟随，eax 内容如下图。



```
地址     HEX 数据                                              ASCII
00A840D0 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 0  MZ?....¦...ÿÿ..
00A840E0 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 0  ?.......@.......
00A840F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0  ................
00A84100 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0  ..............£.
00A84110 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 6  ■■?.???L?Th
00A84120 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6  is program canno
00A84130 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 2  t be run in DOS
00A84140 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 0  mode....$.......
00A84150 BB 26 36 59 FF 47 58 0A FF 47 58 0A FF 47 58 0  ?6YÿGX.ÿGX.ÿGX.
00A84160 F6 3F CB 0A F5 47 58 0A 1A 1E 59 0B FD 47 58 0  ??鲜X.■■Y■劃X.
00A84170 1A 1E 5B 0B FC 47 58 0A 1A 1E 5D 0B EA 47 58 0A ■■[■觊X.■■]■圕X.
00A84180 1A 1E 5C 0B F4 47 58 0A 22 B8 96 0A FA 47 58 0A ■■\■鐾X."笘.鶡X.
00A84190 22 B8 93 0A F6 47 58 0A FF 47 59 0A BA 47 58 0A "铊.鰑X.ÿGY.篏X.
00A841A0 0D 1E 51 0B FB 47 58 0A 0D 1E 58 0B FE 47 58 0A .■Q■髗X..■X■剥X.
```

由此猜测 atidrv.dll 这个 dll 是静态加载的。

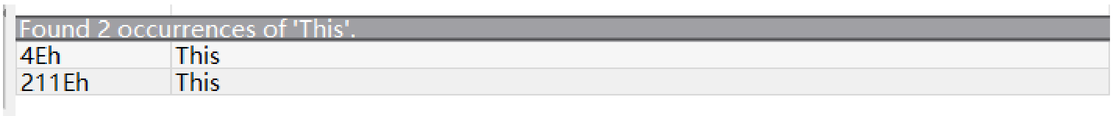
当运行至资源加载完毕后，可以看到在 c 盘 Windows 文件夹下出现了 atidrv.dll。



› 此电脑 › Windows (C:) › Windows　　搜索"Windows"

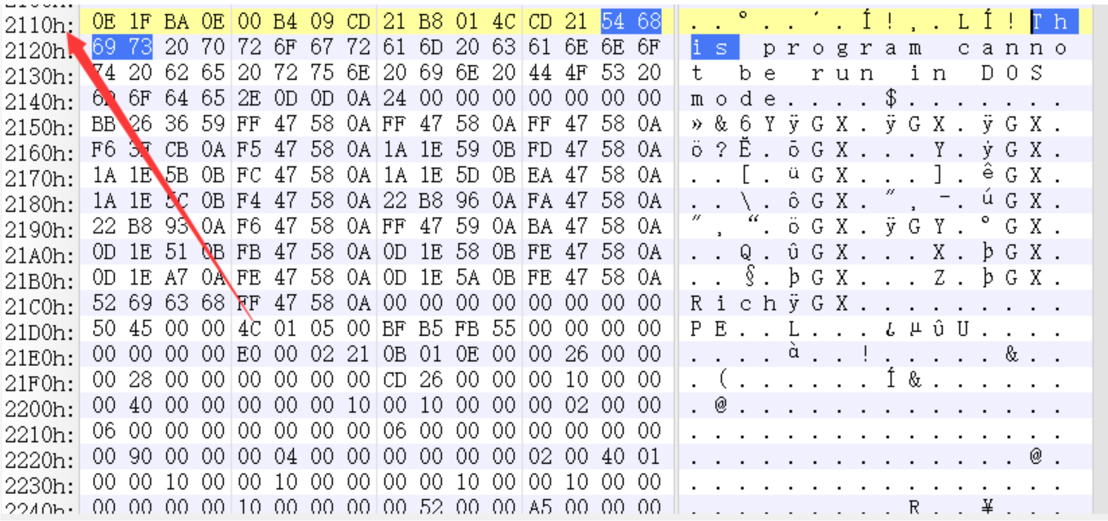
□ 名称	修改日期	类型	大小
[redacted]	[redacted]/11/27 12:31	79ST9 文件	287 KB
[redacted]	[redacted]/4 17:35	PALGZ 文件	136 KB
[redacted]	2017/6/10 14:46	15BY 文件	143 KB
[redacted]	2017/11/26 20:10	18NGI 文件	101 KB
[redacted]	2019/1/20 10:43	Windows 批处理...	1 KB
[redacted]	2019/1/20 10:47	Executable Jar File	10,746 KB
☑ atidrv.dll	2019/4/7 20:34	应用程序扩展	20 KB

最后，用 010editor 打开恶意程序 Lab_03-1.malware 与 atidrv.dll 进行对比。在 malware 文件中搜索 atidrv.dll 的开头 This 字样，如下图。



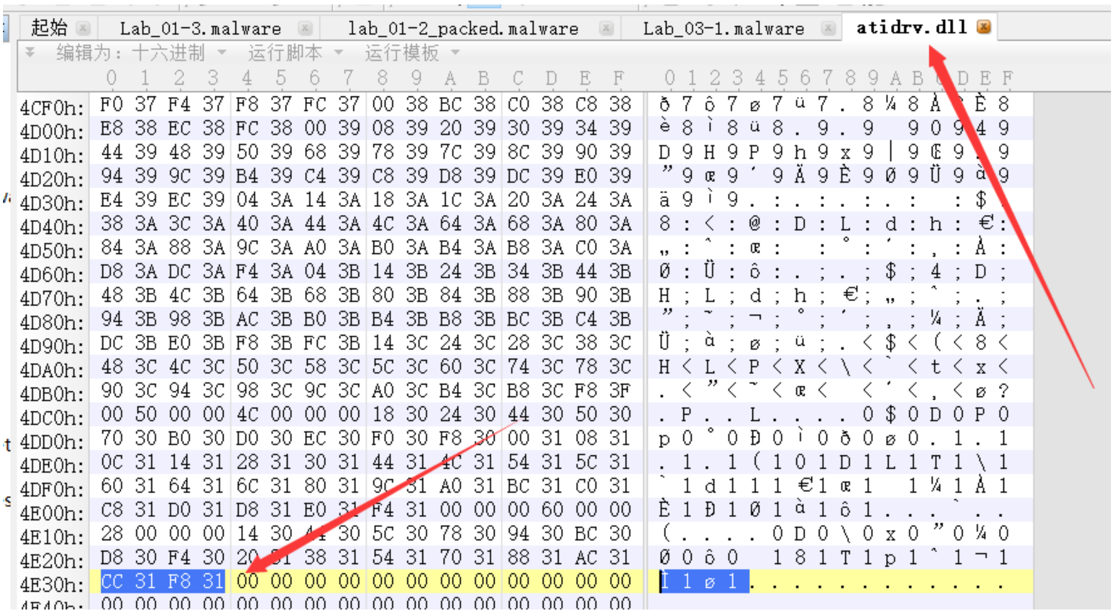
Found 2 occurrences of 'This'.

4Eh	This
211Eh	This

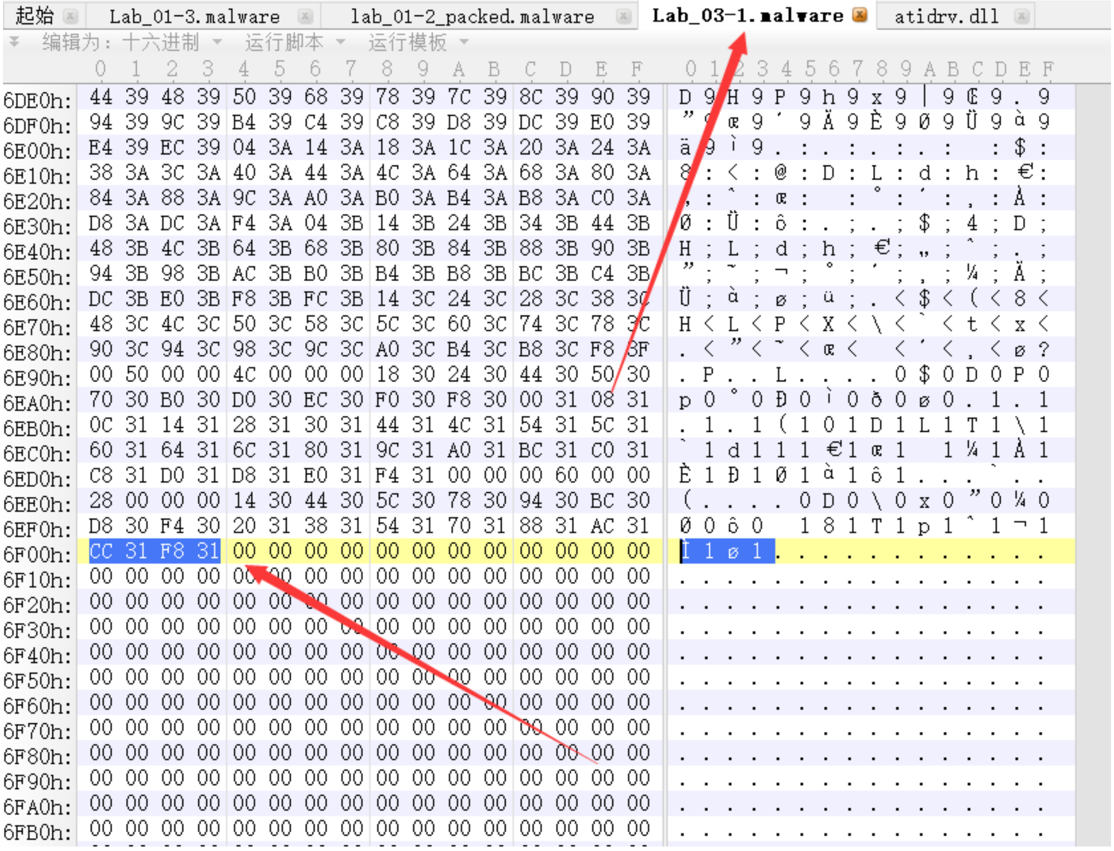


```
2110h: 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  ..º..´.Í!¸.LÍ!Th
2120h: 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is program canno
2130h: 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  t be run in DOS 
2140h: 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00  mode....$.......
2150h: BB 26 36 59 FF 47 58 0A FF 47 58 0A FF 47 58 0A  »&6YÿGX.ÿGX.ÿGX.
2160h: F6 3F CB 0A F5 47 58 0A 1A 1E 59 0B FD 47 58 0A  ö?Ë.õGX...Y.ýGX.
2170h: 1A 1E 5B 0B FC 47 58 0A 1A 1E 5D 0B EA 47 58 0A  ..[.üGX...].êGX.
2180h: 1A 1E 5C 0B F4 47 58 0A 22 B8 96 0A FA 47 58 0A  ..\.ôGX."¸–.úGX.
2190h: 22 B8 93 0A F6 47 58 0A FF 47 59 0A BA 47 58 0A  "¸“.öGX.ÿGY.ºGX.
21A0h: 0D 1E 51 0B FB 47 58 0A 0D 1E 58 0B FE 47 58 0A  ..Q.ûGX...X.þGX.
21B0h: 0D 1E A7 0A FE 47 58 0A 0D 1E 5A 0B FE 47 58 0A  ..§.þGX...Z.þGX.
21C0h: 52 69 63 68 FF 47 58 0A 00 00 00 00 00 00 00 00  RichÿGX.........
21D0h: 50 45 00 00 4C 01 05 00 BF B5 FB 55 00 00 00 00  PE..L...¿µûU....
21E0h: 00 00 00 00 E0 00 02 21 0B 01 0E 00 00 26 00 00  ....à..!.....&..
21F0h: 00 28 00 00 00 00 00 00 CD 26 00 00 00 10 00 00  .(......Í&......
2200h: 00 40 00 00 00 00 00 10 00 10 00 00 00 02 00 00  .@..............
2210h: 06 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00  ................
2220h: 00 90 00 00 00 04 00 00 00 00 00 00 02 00 40 01  ..............@.
2230h: 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00  ................
2240h: 00 00 00 00 10 00 00 00 00 52 00 00 A5 00 00 00  .........R..¥...
```

搜索 atidrv.dll 的末尾



```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
4CF0h: F0 37 F4 37 F8 37 FC 37 00 38 BC 38 C0 38 C8 38  ð7ô7ø7ü7.8¼8À8È8
4D00h: E8 38 EC 38 FC 38 00 39 08 39 20 39 30 39 34 39  è8ì8ü8.9.9 90949
4D10h: 44 39 48 39 50 39 68 39 78 39 7C 39 8C 39 90 39  D9H9P9h9x9|9Œ9.9
4D20h: 94 39 9C 39 B4 39 C4 39 C8 39 D8 39 DC 39 E0 39  ”9œ9´9Ä9È9Ø9Ü9à9
4D30h: E4 39 EC 39 04 3A 14 3A 18 3A 1C 3A 20 3A 24 3A  ä9ì9.:.:.:.: :$:
4D40h: 38 3A 3C 3A 40 3A 44 3A 4C 3A 64 3A 68 3A 80 3A  8:<:@:D:L:d:h:€:
4D50h: 84 3A 88 3A 9C 3A A0 3A B0 3A B4 3A B8 3A C0 3A  „:ˆ:œ: :°:´:¸:À:
4D60h: D8 3A DC 3A F4 3A 04 3B 14 3B 24 3B 34 3B 44 3B  Ø:Ü:ô:.;.;$;4;D;
4D70h: 48 3B 4C 3B 64 3B 68 3B 80 3B 84 3B 88 3B 90 3B  H;L;d;h;€;„;ˆ;.;
4D80h: 94 3B 98 3B AC 3B B0 3B B4 3B B8 3B BC 3B C4 3B  ”;˜;¬;°;´;¸;¼;Ä;
4D90h: DC 3B E0 3B F8 3B FC 3B 14 3C 24 3C 28 3C 38 3C  Ü;à;ø;ü;.<$<(<8<
4DA0h: 48 3C 4C 3C 50 3C 58 3C 5C 3C 60 3C 74 3C 78 3C  H<L<P<X<\<`<t<x<
4DB0h: 90 3C 94 3C 98 3C 9C 3C A0 3C B4 3C B8 3C F8 3F  .<”<˜<œ< <´<¸<ø?
4DC0h: 00 50 00 00 4C 00 00 00 18 30 24 30 44 30 50 30  .P..L....0$0D0P0
4DD0h: 70 30 B0 30 D0 30 EC 30 F0 30 F8 30 00 31 08 31  p0°0Ð0ì0ð0ø0.1.1
4DE0h: 0C 31 14 31 28 31 30 31 44 31 4C 31 54 31 5C 31  .1.1(101D1L1T1\1
4DF0h: 60 31 64 31 6C 31 80 31 9C 31 A0 31 BC 31 C0 31  `1d1l1€1œ1 1¼1À1
4E00h: C8 31 D0 31 D8 31 E0 31 F4 31 00 00 00 60 00 00  È1Ð1Ø1à1ô1...`..
4E10h: 28 00 00 00 14 30 44 30 5C 30 78 30 94 30 BC 30  (....0D0\0x0”0¼0
4E20h: D8 30 F4 30 20 31 38 31 54 31 70 31 88 31 AC 31  Ø0ô0 181T1p1ˆ1¬1
4E30h: CC 31 F8 31 00 00 00 00 00 00 00 00 00 00 00 00  Ì1ø1............
4E40h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```



```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
6DE0h: 44 39 48 39 50 39 68 39 78 39 7C 39 8C 39 90 39   D9H9P9h9x9|9Œ9.9
6DF0h: 94 39 9C 39 B4 39 C4 39 C8 39 D8 39 DC 39 E0 39   ”9œ9´9Ä9È9Ø9Ü9à9
6E00h: E4 39 EC 39 04 3A 14 3A 18 3A 1C 3A 20 3A 24 3A   ä9ì9.:.:.:.: :$:
6E10h: 38 3A 3C 3A 40 3A 44 3A 4C 3A 64 3A 68 3A 80 3A   8:<:@:D:L:d:h:€:
6E20h: 84 3A 88 3A 9C 3A A0 3A B0 3A B4 3A B8 3A C0 3A   „:ˆ:œ: :°:´:¸:À:
6E30h: D8 3A DC 3A F4 3A 04 3B 14 3B 24 3B 34 3B 44 3B   Ø:Ü:ô:.;.;$;4;D;
6E40h: 48 3B 4C 3B 64 3B 68 3B 80 3B 84 3B 88 3B 90 3B   H;L;d;h;€;„;ˆ;.;
6E50h: 94 3B 98 3B AC 3B B0 3B B4 3B B8 3B BC 3B C4 3B   ”;˜;¬;°;´;¸;¼;Ä;
6E60h: DC 3B E0 3B F8 3B FC 3B 14 3C 24 3C 28 3C 38 3C   Ü;à;ø;ü;.<$<(<8<
6E70h: 48 3C 4C 3C 50 3C 58 3C 5C 3C 60 3C 74 3C 78 3C   H<L<P<X<\<`<t<x<
6E80h: 90 3C 94 3C 98 3C 9C 3C A0 3C B4 3C B8 3C F8 3F   .<”<˜<œ< <´<¸<ø?
6E90h: 00 50 00 00 4C 00 00 00 18 30 24 30 44 30 50 30   .P..L....0$0D0P0
6EA0h: 70 30 B0 30 D0 30 EC 30 F0 30 F8 30 00 31 08 31   p0°0Ð0ì0ð0ø0.1.1
6EB0h: 0C 31 14 31 28 31 30 31 44 31 4C 31 54 31 5C 31   .1.1(101D1L1T1\1
6EC0h: 60 31 64 31 6C 31 80 31 9C 31 A0 31 BC 31 C0 31   `1d1l1€1œ1 1¼1À1
6ED0h: C8 31 D0 31 D8 31 E0 31 F4 31 00 00 00 60 00 00   È1Ð1Ø1à1ô1...`..
6EE0h: 28 00 00 00 14 30 44 30 5C 30 78 30 94 30 BC 30   (....0D0\0x0”0¼0
6EF0h: D8 30 F4 30 20 31 38 31 54 31 70 31 88 31 AC 31   Ø0ô0 181T1p1ˆ1¬1
6F00h: CC 31 F8 31 00 00 00 00 00 00 00 00 00 00 00 00   Ì1ø1............
6F10h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
6F20h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
6F30h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
6F40h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
6F50h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
6F60h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
6F70h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
6F80h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
6F90h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
6FA0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
6FB0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
```

于是该资源也可以直接 dump 出来。

2. (3 pts) List at least 3 imports or sets of imports. What is their purpose (from msdn), and how might the malware use them?

a. FindResourceW 获取自定义资源

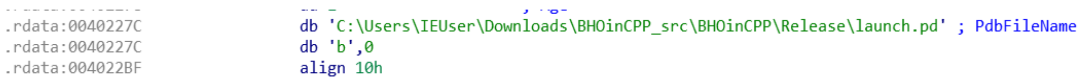
b. CreateFileW 写文件

c. system 执行命令

3. (3 pts) List at least 3 strings that stick out to you and describe how they might relate to malicious activity.

a. regsvr32 /s C:\Windows\atidrv.dll 注册 dll，从而进行后续操作

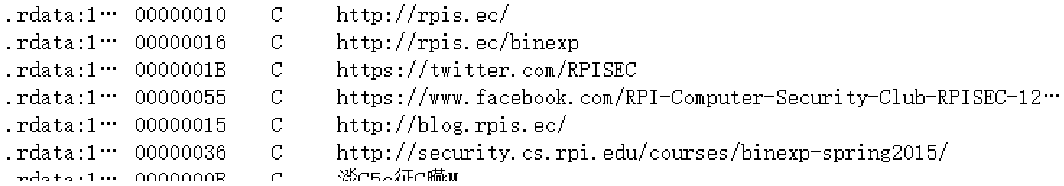
b.



```
.rdata:0040227C                 db 'C:\Users\IEUser\Downloads\BHOinCPP_src\BHOinCPP\Release\launch.pd' ; PdbFileName
.rdata:0040227C                 db 'b',0
.rdata:004022BF                 align 10h
```

潜在资源

c. 存在多个 url 链接，可能进行网络操作



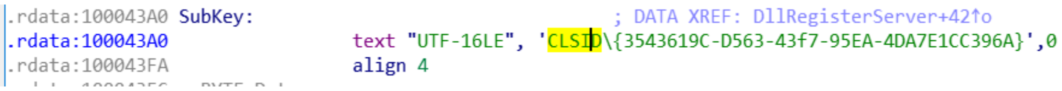
```
.rdata:1…  00000010   C    http://rpis.ec/
.rdata:1…  00000016   C    http://rpis.ec/binexp
.rdata:1…  0000001B   C    https://twitter.com/RPISEC
.rdata:1…  00000055   C    https://www.facebook.com/RPI-Computer-Security-Club-RPISEC-12…
.rdata:1…  00000015   C    http://blog.rpis.ec/
.rdata:1…  00000036   C    http://security.cs.rpi.edu/courses/binexp-spring2015/
```

4. (3 pts) What persistence mechanism is used by this malware? What host-based signatures can you gather from this?

该恶意程序将加载在自身里的 dll 写入主机，并注册该 dll。

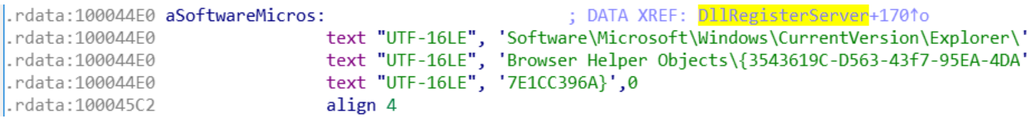
5. (2 pts) What is the CLSID served by this malware?

在 dump 出来的 dll 文件中可以查到，{3543619C-D563-43f7-95EA-4DA7E1CC396A}



```
.rdata:100043A0 SubKey:                         ; DATA XREF: DllRegisterServer+42↑o
.rdata:100043A0                 text "UTF-16LE", 'CLSID\{3543619C-D563-43f7-95EA-4DA7E1CC396A}',0
.rdata:100043FA                 align 4
```

6. (2 pts) What is the name of the COM interface that this malware makes use of?

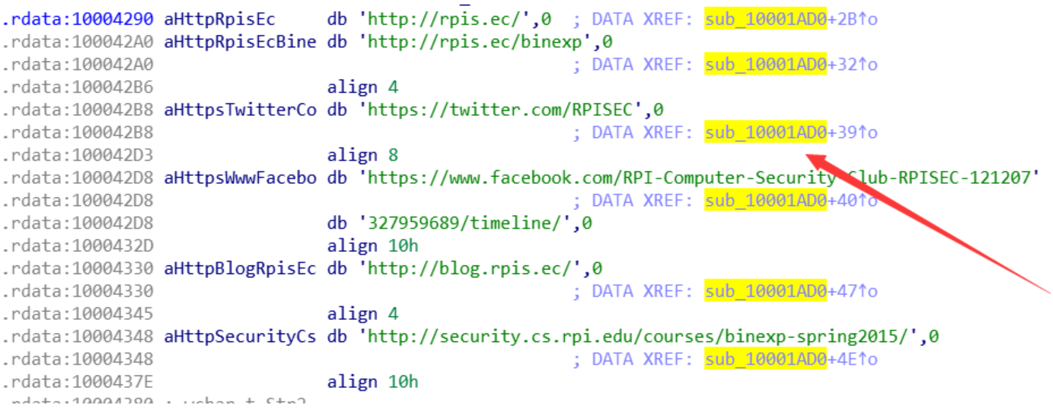


```
.rdata:100044E0 aSoftwareMicros:                       ; DATA XREF: DllRegisterServer+170↑o
.rdata:100044E0                 text "UTF-16LE", 'Software\Microsoft\Windows\CurrentVersion\Explorer\'
.rdata:100044E0                 text "UTF-16LE", 'Browser Helper Objects\{3543619C-D563-43f7-95EA-4DA'
.rdata:100044E0                 text "UTF-16LE", '7E1CC396A}',0
.rdata:100045C2                 align 4
```

7. (2 pts) What two COM functions does this malware call from the above COM interface, and what are they used for? (hint: check the PMA book)

IwebBrowser

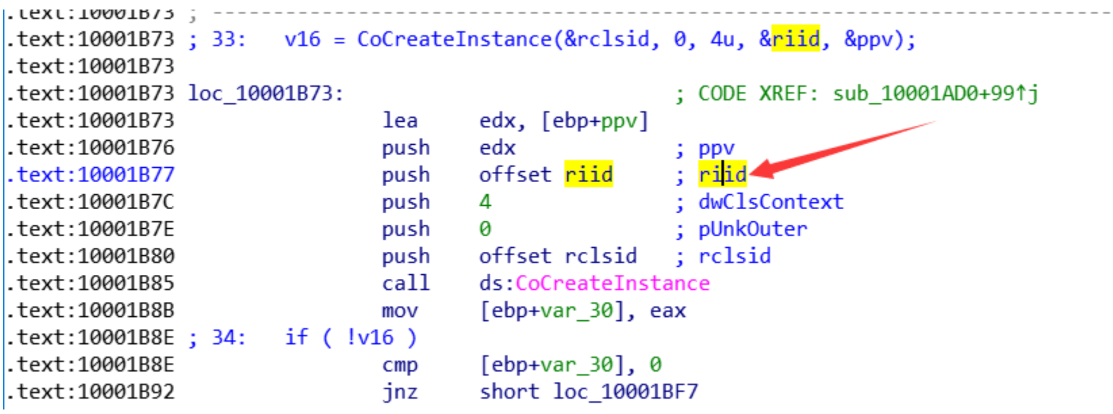
通过 url 可定位至相应函数。



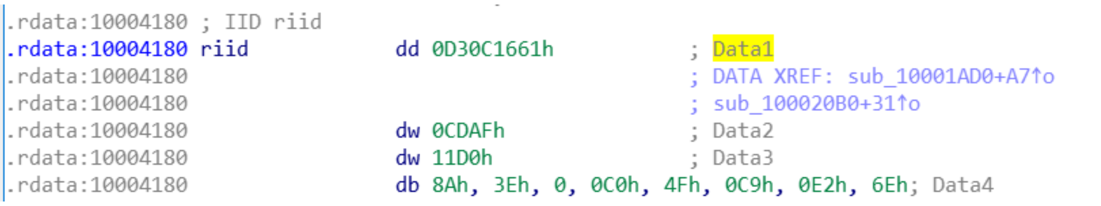
```
.rdata:10004290 aHttpRpisEc     db 'http://rpis.ec/',0  ; DATA XREF: sub_10001AD0+2B↑o
.rdata:100042A0 aHttpRpisEcBine db 'http://rpis.ec/binexp',0
.rdata:100042A0                                         ; DATA XREF: sub_10001AD0+32↑o
.rdata:100042B6                 align 4
.rdata:100042B8 aHttpsTwitterCo db 'https://twitter.com/RPISEC',0
.rdata:100042B8                                         ; DATA XREF: sub_10001AD0+39↑o
.rdata:100042D3                 align 8
.rdata:100042D8 aHttpsWwwFacebo db 'https://www.facebook.com/RPI-Computer-Security-Club-RPISEC-121207'
.rdata:100042D8                                         ; DATA XREF: sub_10001AD0+40↑o
.rdata:100042D8                 db '327959689/timeline/',0
.rdata:1000432D                 align 10h
.rdata:10004330 aHttpBlogRpisEc db 'http://blog.rpis.ec/',0
.rdata:10004330                                         ; DATA XREF: sub_10001AD0+47↑o
.rdata:10004345                 align 4
.rdata:10004348 aHttpSecurityCs db 'http://security.cs.rpi.edu/courses/binexp-spring2015/',0
.rdata:10004348                                         ; DATA XREF: sub_10001AD0+4E↑o
.rdata:1000437E                 align 10h
```

如下，riid 参数为 D30C1661，百度查到是 IwebBrowser

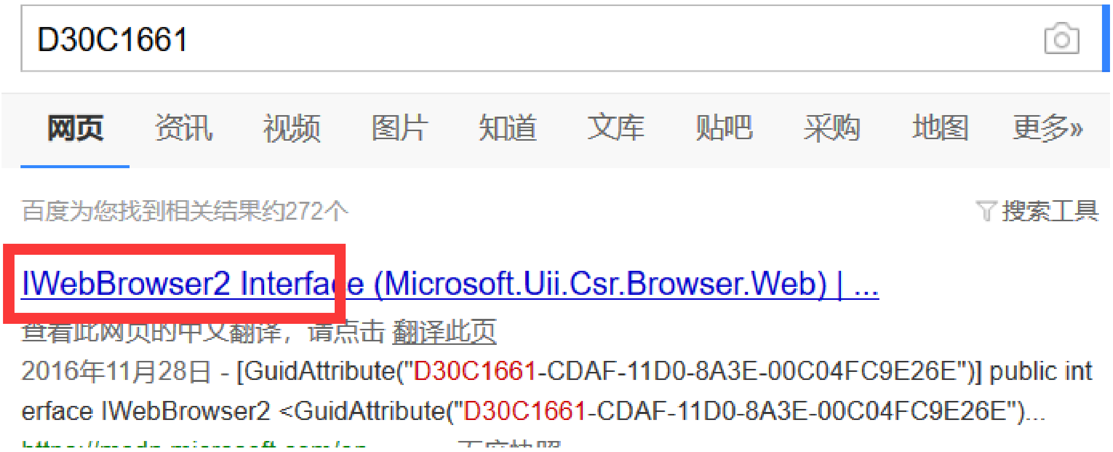
的参数



```
.text:10001B73 ; ---------------------------------------------------------------
.text:10001B73 ; 33:   v16 = CoCreateInstance(&rclsid, 0, 4u, &riid, &ppv);
.text:10001B73
.text:10001B73 loc_10001B73:                           ; CODE XREF: sub_10001AD0+99↑j
.text:10001B73                 lea     edx, [ebp+ppv]
.text:10001B76                 push    edx             ; ppv
.text:10001B77                 push    offset riid     ; riid
.text:10001B7C                 push    4               ; dwClsContext
.text:10001B7E                 push    0               ; pUnkOuter
.text:10001B80                 push    offset rclsid   ; rclsid
.text:10001B85                 call    ds:CoCreateInstance
.text:10001B8B                 mov     [ebp+var_30], eax
.text:10001B8E ; 34:   if ( !v16 )
.text:10001B8E                 cmp     [ebp+var_30], 0
.text:10001B92                 jnz     short loc_10001BF7
```



```
.rdata:10004180 ; IID riid
.rdata:10004180 riid            dd 0D30C1661h           ; Data1
.rdata:10004180                                         ; DATA XREF: sub_10001AD0+A7↑o
.rdata:10004180                                         ; sub_100020B0+31↑o
.rdata:10004180                 dw 0CDAFh               ; Data2
.rdata:10004180                 dw 11D0h                ; Data3
.rdata:10004180                 db 8Ah, 3Eh, 0, 0C0h, 4Fh, 0C9h, 0E2h, 6Eh; Data4
```



D30C1661

百度为您找到相关结果约272个

IWebBrowser2 Interface (Microsoft.Uii.Csr.Browser.Web) | ...

查看此网页的中文翻译，请点击 翻译此页

2016年11月28日 - [GuidAttribute("D30C1661-CDAF-11D0-8A3E-00C04FC9E26E")] public interface IWebBrowser2 <GuidAttribute("D30C1661-CDAF-11D0-8A3E-00C04FC9E26E")...

Lab_03-2

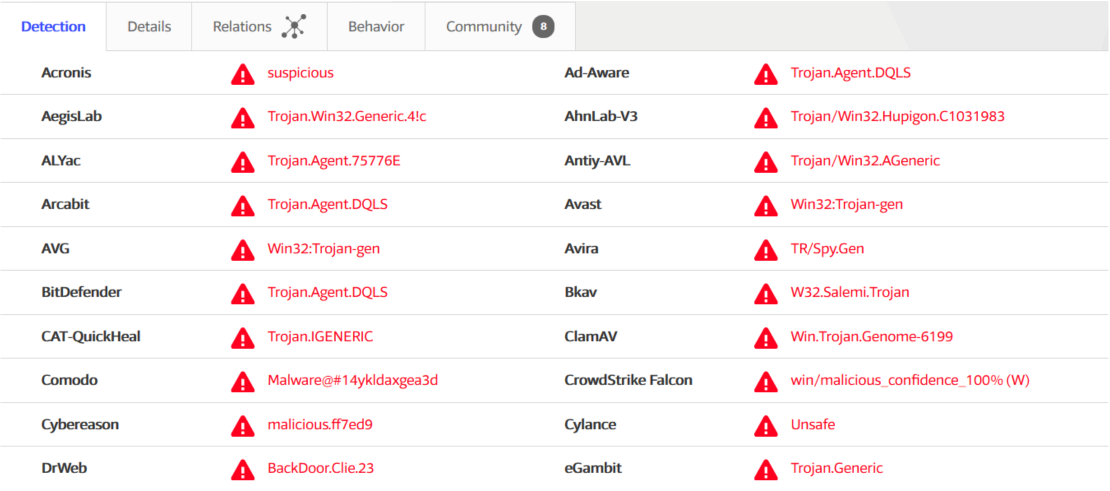
Basic Analysis

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

Md5sum 如下

MD5	bf4f5b4ff7ed9c7275496c07f9836028

Virtustotal 结果如下



Acronis	suspicious	Ad-Aware	Trojan.Agent.DQLS
AegisLab	Trojan.Win32.Generic.4!c	AhnLab-V3	Trojan/Win32.Hupigon.C1031983
ALYac	Trojan.Agent.75776E	Antiy-AVL	Trojan/Win32.AGeneric
Arcabit	Trojan.Agent.DQLS	Avast	Win32:Trojan-gen
AVG	Win32:Trojan-gen	Avira	TR/Spy.Gen
BitDefender	Trojan.Agent.DQLS	Bkav	W32.Salemi.Trojan
CAT-QuickHeal	Trojan.IGENERIC	ClamAV	Win.Trojan.Genome-6199
Comodo	Malware@#14ykldaxgea3d	CrowdStrike Falcon	win/malicious_confidence_100% (W)
Cybereason	malicious.ff7ed9	Cylance	Unsafe
DrWeb	BackDoor.Clie.23	eGambit	Trojan.Generic

2. (3 pts) List at least 3 imports or sets of imports you haven’t seen before, what is their purpose (from msdn), and how might the malware use them.

a. Process32Next

进程获取函数

b. TerminateProcess

终止指定的进程及其所有线程

c. FreeEnvironmentStringsA

释放指定的环境字串块

3. (3 pts) List at least 3 strings that stick out to you and describe how they might relate to malicious activity.

a. SOFTWARE\Microsoft\Windows\CurrentVersion\Run

通过该字符串获取主机注册表中的开机启动项，并将程序写入注册表。

b. 127.0.0.1

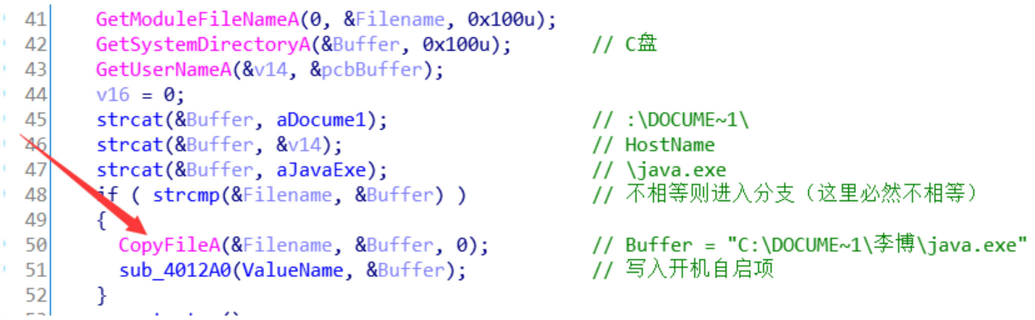
获取本机 localhost 的 IP 地址，然后与 127.0.0.1 比较

c. \java.exe

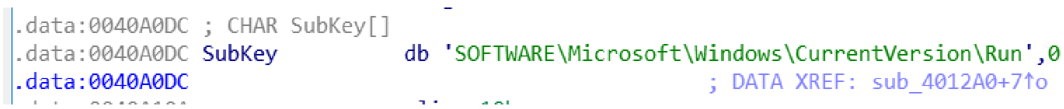
获取系统 java 环境

4. (3 pts) What persistence mechanism is used by this malware? What host-based signatures can you gather from this?

该程序通过将自身复制至系统文件夹（**C:\DOCUME~1\李博\java.exe**），并写入注册表中的开机启动项达到持久性运行的目的。



```
    GetModuleFileNameA(0, &Filename, 0x100u);
    GetSystemDirectoryA(&Buffer, 0x100u);        // C盘
    GetUserNameA(&v14, &pcbBuffer);
    v16 = 0;
    strcat(&Buffer, aDocume1);                   // :\DOCUME~1\
    strcat(&Buffer, &v14);                       // HostName
    strcat(&Buffer, aJavaExe);                   // \java.exe
    if ( strcmp(&Filename, &Buffer) )            // 不相等则进入分支（这里必然不相等）
    {
      CopyFileA(&Filename, &Buffer, 0);          // Buffer = "C:\DOCUME~1\李博\java.exe"
      sub_4012A0(ValueName, &Buffer);            // 写入开机自启项
    }
```



```
.data:0040A0DC ; CHAR SubKey[]
.data:0040A0DC SubKey          db 'SOFTWARE\Microsoft\Windows\CurrentVersion\Run',0
.data:0040A0DC                                         ; DATA XREF: sub_4012A0+7↑o
```

Advanced Analysis

5. (1 pts) What is the address of the subroutine that handles this functionality?

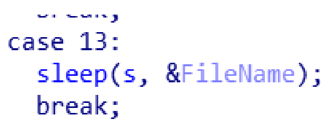
a. 0x004028C0 sleep

b. 0x00401A20 上传文件

c. 0x00402050 调用 WinExec 运行程序并返回 0（失败）或 1（成功）

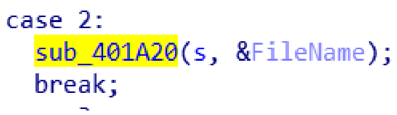
6. (1 pts) What is the command ID? It will help the networking guys group the traffic.

a. ID: 0xD(13) - 0x004028C0



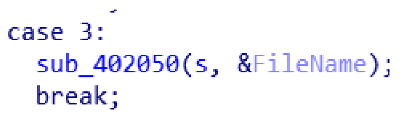
```
case 13:
  sleep(s, &FileName);
  break;
```

b. ID: 2 - 0x00401A20



```
case 2:
  sub_401A20(s, &FileName);
  break;
```

c. ID: 3 - 0x00402050



```
case 3:
  sub_402050(s, &FileName);
  break;
```

7. (1pts) Does the subroutine return anything to the attacker, if so, what?

a. 0x004028C0 - 只有 sleep 操作

b. 0x00401A20 - 将经过 0x55 异或加密过的文件上传给攻击者

c. 0x00402050 - 调用 WinExec 运行程序并返回 0（失败）或 1（成功）给攻击者

8. (3 pts) Name 3 Windows API calls used and how they contribute to the functionality. (send/recv don’t count!)

a. GetLogicalDrives 获取逻辑驱动器个数，便于后续获取盘符

b. FindFirstFileA 获取第一个文件的句柄

c. WinExec 执行程序

9. (3 pts) Did the networking guys miss anything? Briefly name/describe 3 more functionalities

offered by the malware. Provide the command IDs.

a. id=1，获取系统盘符，并发送给攻击者

b. id=4，删除文件，并将删除操作是否成功的返回值发送给攻击者

c. id=5，从攻击者主机接收文件