

Shadow Brokers	NSA	DoublePulsar	
	DoublePulsar		
	SMB	RDP	
	EternalBlue	EternalRomance	srv.sys
SrvTransaction2DispatchTable	14	srv.sys	
SrvTransaction2DispatchTable	14		
SrvTransactionNotImplemented	SMB	SMB_COM_TRANSACTION2	
	DoublePulsar		
SMB_COM_TRANSACTION2			

1. SrvTransaction2DispatchTable

3.DoublePulsar

OutputInstall	shellcode RunShellcode
Ping	DoublePulsar
RunDLL RunShellcode	shellcode Dll



(1)CheckFlag

SMB_COM_TRANSACTION2

```

Timeout      flag
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
seg000:86847198 add     al, cl
seg000:86847198 shr     ecx, 8
seg000:86847198 add     al, cl
seg000:86847198 endp

```

```

timeout      0x23
11 0.005951 192.168.0.101 192.168.0.101 SMB 445 136 Trans2 Request: SECTION_SETUP
15 0.011895 192.168.0.101 192.168.0.101 SMB 445 1312 Trans2 Request: SECTION_SETUP
Max Parameter Count: 1
Max Data Count: 0
Max Setup Count: 0
Reserved: 00
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
0030 3f c9 96 39 00 00 00 00 4e ff 53 4d 42 32 00 ?..9....N.SMB2.
0040 00 00 00 18 07 c0 00 00 00 00 00 00 00 00 00 .....
0050 00 00 00 08 ff fe 00 08 41 00 0f 0c 00 00 01 .....A.....
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....B
0070 00 00 00 4e 00 01 00 0e 00 0d 00 00 00 00 00 .....N.....
0080 00 00 00 00 00 00 00 00

```

0x23	Ping
0x77	
0xc8	shellcode

(

0x77

SrvTransaction2DispatchTable

```
seg000:86847189 sub_86847189 proc near ; CODE XREF: start:loc_868470A1↑p  
seg000:86847180 nusha
```

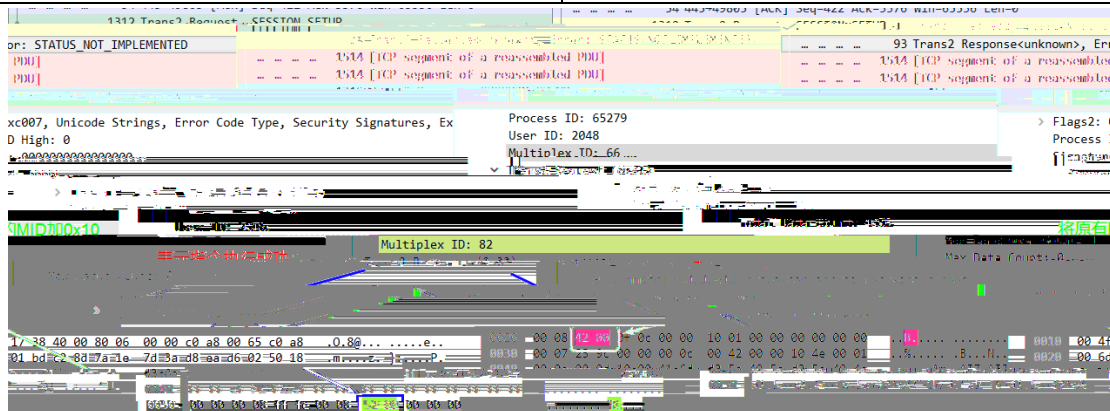
(5)

SrvTransactionNotImplemented

MID

```
seg000:86847140  
seg000:86847140 loc_86847140: ; CODE XREF: start+54↑j  
; CODE XREF: start+41↑j  
; start+7F↑j ...  
; 20h  
ort loc_86847140  
; CODE XREF: start+9B↑j  
; 30h; '0'  
ort $+2  
; CODE XREF: start+FA↑j  
; start+FE↑j ...  
x, [ebp+38h]  
; 0  
cx+1Eh], ax ; add al, 0  
; CODE XREF: start+24↑j  
x, [ebp+10h]  
sp+20h+var_4], eax  
ord ptr [eax+3Ch]; jmp old_SrvTransactionNotImplemented  
seg000:86847148 mov al  
seg000:86847142 jmp sh  
seg000:86847144  
seg000:86847144 loc_86847144:  
seg000:86847144  
seg000:86847146 mov al  
seg000:86847146 jmp sh  
seg000:86847148  
seg000:86847148 loc_86847148:  
seg000:86847148 mov al  
seg000:86847148 jmp sh  
seg000:8684714C  
seg000:8684714C loc_8684714C:  
seg000:8684714C  
seg000:8684714E mov ec  
seg000:8684714E mov ah  
seg000:8684714E add [e  
seg000:86847150  
seg000:86847150 loc_86847150:  
seg000:86847150  
seg000:86847152 mov ea  
seg000:86847152  
seg000:86847154 mov [e  
seg000:86847154  
seg000:86847156 jmp dv  
seg000:86847158  
seg000:86847158
```

MID+0x10	
MID+0x20	
MID+0x30	



VenusEye

VenusEye

Hedwig

Locky

18

Sage 2.0

Office

0day

2016

