

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 .....B
0070 00 00 00 4e 00 01 00 0e 00 0d 00 00 00 00 .....N.....
0080 00 00 00 00 00 00 00 00

```

0x23	Ping
0x77	
0xc8	shellcode

(

[illegible]

```

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+94h] ; PsGetProcessImageFileName

```

[illegible]

(4)Uninstall

VenusEye

VenusEye

Hedwig

Locky

18

Sage 2.0

Office

0day

2016

