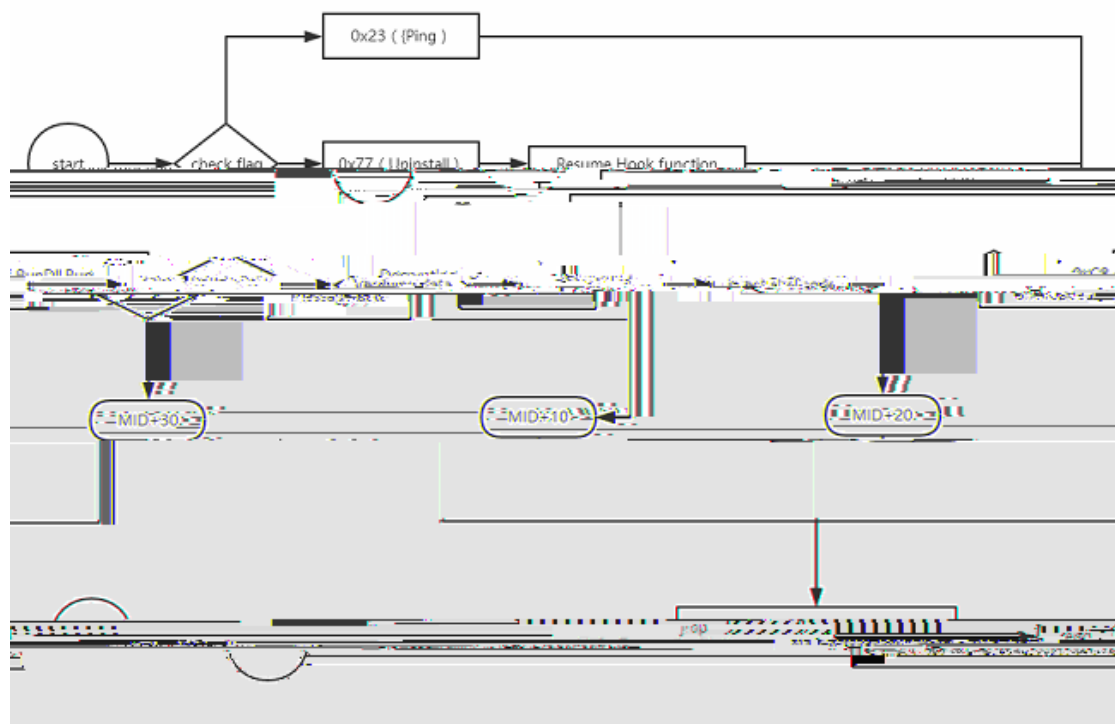


Shadow Brokers	NSA	DoublePulsar	
	DoublePulsar		
	SMB	RDP	
	EternalBlue	EternalRomance	srv.sys
SrvTransaction2DispatchTable	14	srv.sys	
SrvTransaction2DispatchTable	14		
SrvTransactionNotImplemented	SMB	SMB_COM_TRANSACTION2	
	DoublePulsar		
SMB_COM_TRANSACTION2			

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+301p
seg000:86847194 xor     eax, eax
seg000:86847196 mov     al, cl
seg000:86847198 shr     ecx, 8
seg000:86847198 add     al, cl
seg000:8684719D shr     ecx, 8
seg000:868471A0 add     al, cl
seg000:868471A7 endp

```

timeout

0x23

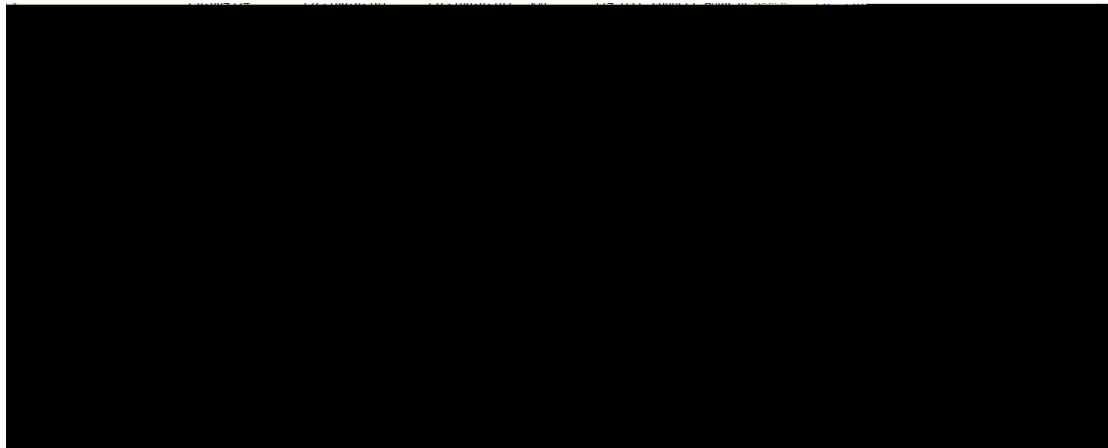
10	0:005892	192.168.0.109	192.168.0.101	SMB	445	136	Trans2 Request, SESSION_SETUP
11	0:005951	192.168.0.101	192.168.0.109	SMB	445	137	Trans2 Response, SESSION_SETUP
15	0:011895	192.168.0.109	192.168.0.101	SMB	445	1312	Trans2 Request, SESSION_SETUP
16	0:011954	192.168.0.101	192.168.0.109	SMB	445	1313	Trans2 Response, SESSION_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

3f c9 96 39 00 00 00 00 00 4e ff 53 4d 42 32 00H.SMB2
00 00 00 18 07 c0 00 00 00 00 00 00 00 00 00 00
00 00 00 00 ff fa 00 00 41 00 0f 0c 00 00 00 01A
00 00 00 00 00 00 00 00 00 00 0c 00 00 42B
00 00 00 4e 00 01 00 0e 00 0d 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0x23	Ping
0x77	
0xc8	shellcode

(



SESSION_SETUP Data

```
shellcode
```

a. `shellcode`

```

seg000:868470B1      mov     edi, [eax+edx] ; 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]

```

```
b.          shellcode
```

```
shellcode
```

```
shellcode
```

[illegible]

[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
seg000:866F935B      call    dword ptr [edi+30h] ; PsGetProcessImageFileName

```

[illegible]

(4)Uninstall

VenusEye

VenusEye

Hedwig

Locky

18

Sage 2.0

Office

0day

2016

