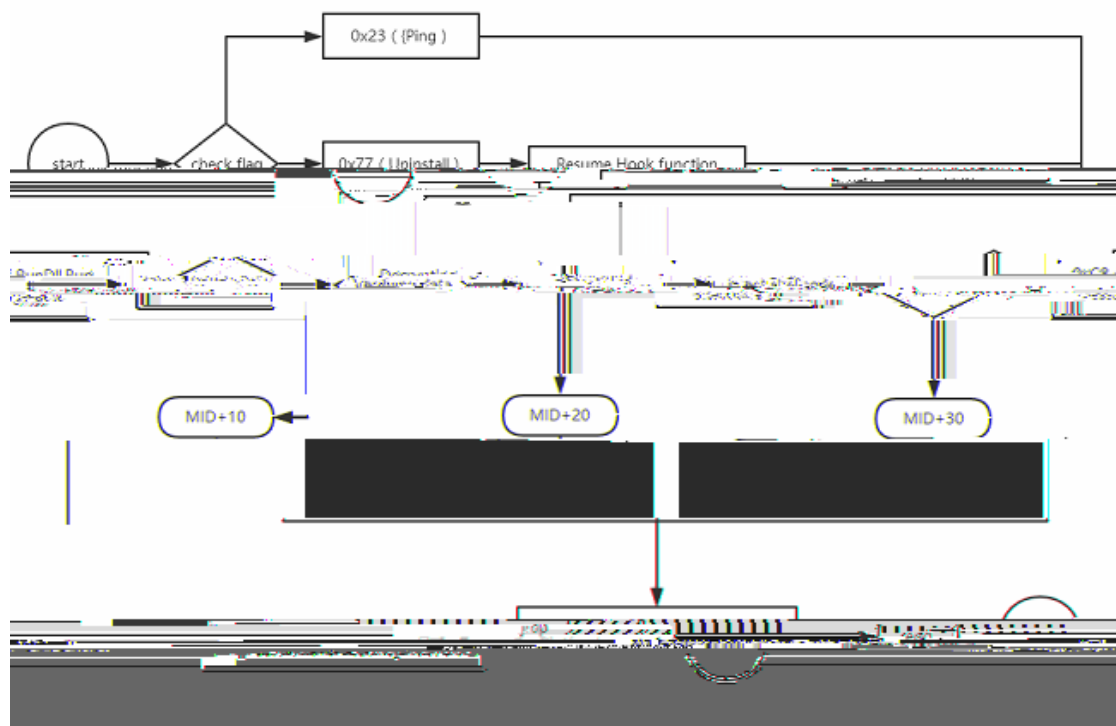


3.DoublePulsar

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
seg000:8684719D shr     ecx, 8
seg000:868471A0 add     al, cl
seg000:868471A7 ret
seg000:868471A7 sub_86847194 endp
seg000:868471A7

```

timeout

0x23

Time	Source	Destination	Protocol	Length	Info
0.005892	192.168.0.109	192.168.0.101	SMB	445	136 Trans2 Request, SESSION_SETUP
0.005951	192.168.0.101	192.168.0.109	SMB	445	136 Trans2 Response, Error: STATUS_NOT_IMPLEMENTED
0.011895	192.168.0.109	192.168.0.101	SMB	445	1312 Trans2 Request, SESSION_SETUP
0.011968	192.168.0.101	192.168.0.109	SMB	445	1312 Trans2 Response, Error: STATUS_NOT_IMPLEMENTED
0.013317	192.168.0.109	192.168.0.101	SMB	445	1312 Trans2 Request, SESSION_SETUP
0.013317	192.168.0.101	192.168.0.109	SMB	445	1312 Trans2 Response, Error: STATUS_NOT_IMPLEMENTED

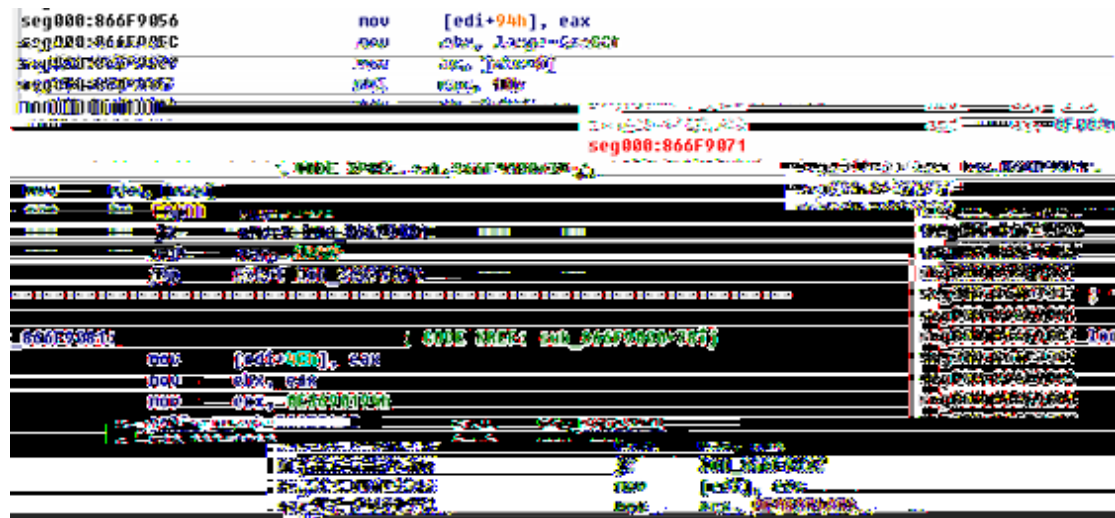
Max Parameter Count:	1
Max Data Count:	0
Max Setup Count:	0
Reserved:	00
Flags:	0x0000
Timeout:	2 hours, 50 minutes, 33.186 seconds
Reserved:	0000
Parameter Count:	12
Parameter Offset:	66
Data Count:	0
Data Offset:	78
Setup Count:	1
Reserved:	00

0030	3f c9 96 39 00 00 00 00 00 4e ff 53 4d	42 32 00	?...N.SMB2
0040	00 00 00 18 07 c0 00 00 00 00 00 00 00 00 00 00		...
0050	00 00 00 08 ff fe 00 08 41 00 0f 0c 00 00 00 01		...A...
0060	00 00 00 00 00 00 00 00 00 00 00 0c 00 42		...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		...

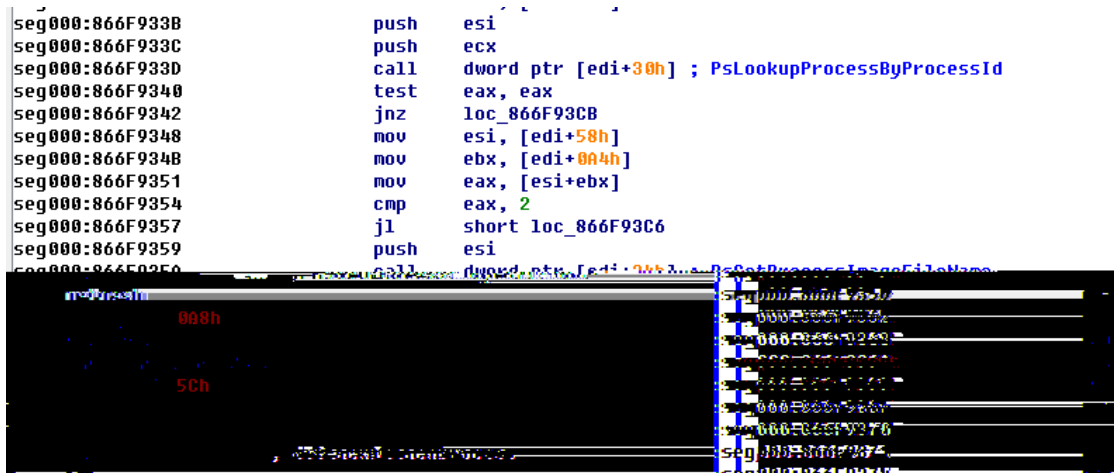
0x23	Ping
0x77	
0xc8	shellcode

(

c. Rundll shellcode IDT ntoskrnl.exe
 IDT ntoskrnl.exe PE



d. PID lsass.exe



e. APC



(4)Uninstall

VenusEye

VenusEye

Hedwig

Locky

18

Sage 2.0

Office

0day

2016

