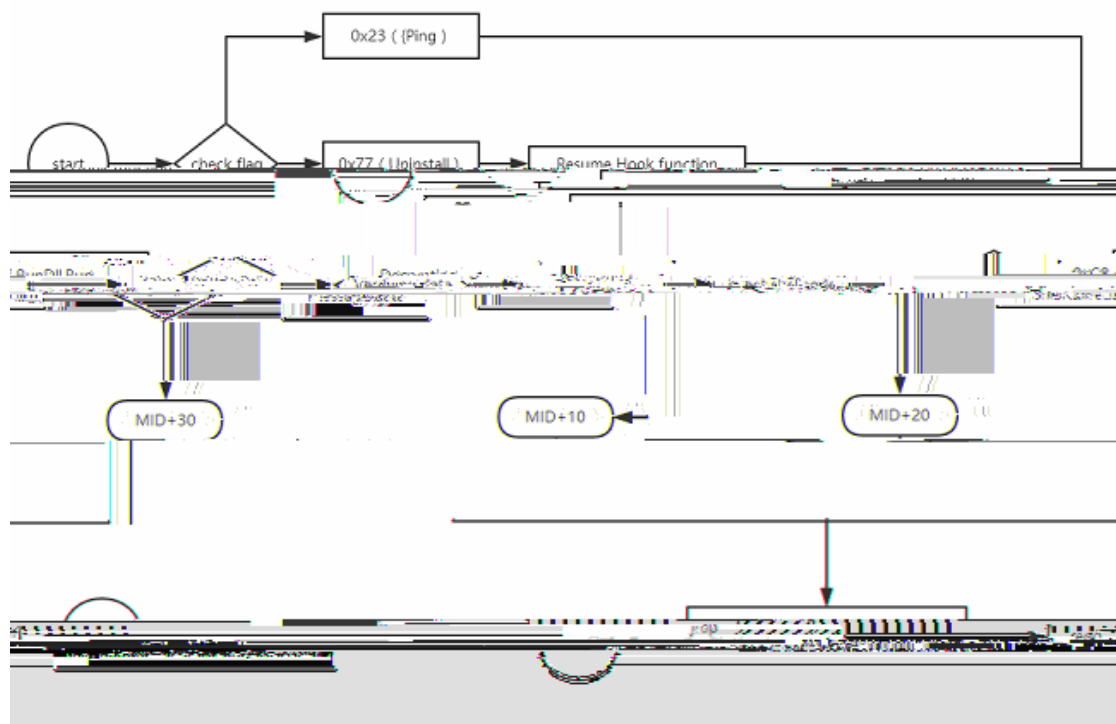


3.DoublePulsar

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
seg000:86847198 shr     ecx, 8
seg000:86847198 add     al, cl
seg000:86847198 ret
sub_86847194 endp
seg000:868471A7

```

timeout 0x23

10 0.005892	192.168.0.109	192.168.0.101	SMB	445	136 Trans2 Request, SECTION_NAME_SETUP
11 0.005951	192.168.0.101	192.168.0.109	SMB	445	136 Trans2 Response, STATUS_SUCCESS, EAX=0, ECX=0, EDI=0, ESI=0, EIP=0, EBP=0, ESP=0, EAX=0, ECX=0, EDI=0, ESI=0, EIP=0, EBP=0, ESP=0
15 0.011895	192.168.0.109	192.168.0.101	SMB	445	1312 Trans2 Request, SEW% & %
16 0.011954	192.168.0.101	192.168.0.109	SMB	445	1312 Trans2 Response, STATUS_SUCCESS, EAX=0, ECX=0, EDI=0, ESI=0, EIP=0, EBP=0, ESP=0, EAX=0, ECX=0, EDI=0, ESI=0, EIP=0, EBP=0, ESP=0

0x23	Ping
0x77	
0xc8	shellcode

(

[illegible]

```

d. PID lsass.exe

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+004h]
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+004h] ; PsGetProcessImageFileName

```

[illegible]

(4)Uninstall

VenusEye

VenusEye

Hedwig

Locky

18

Sage 2.0

Office Oday

2016

