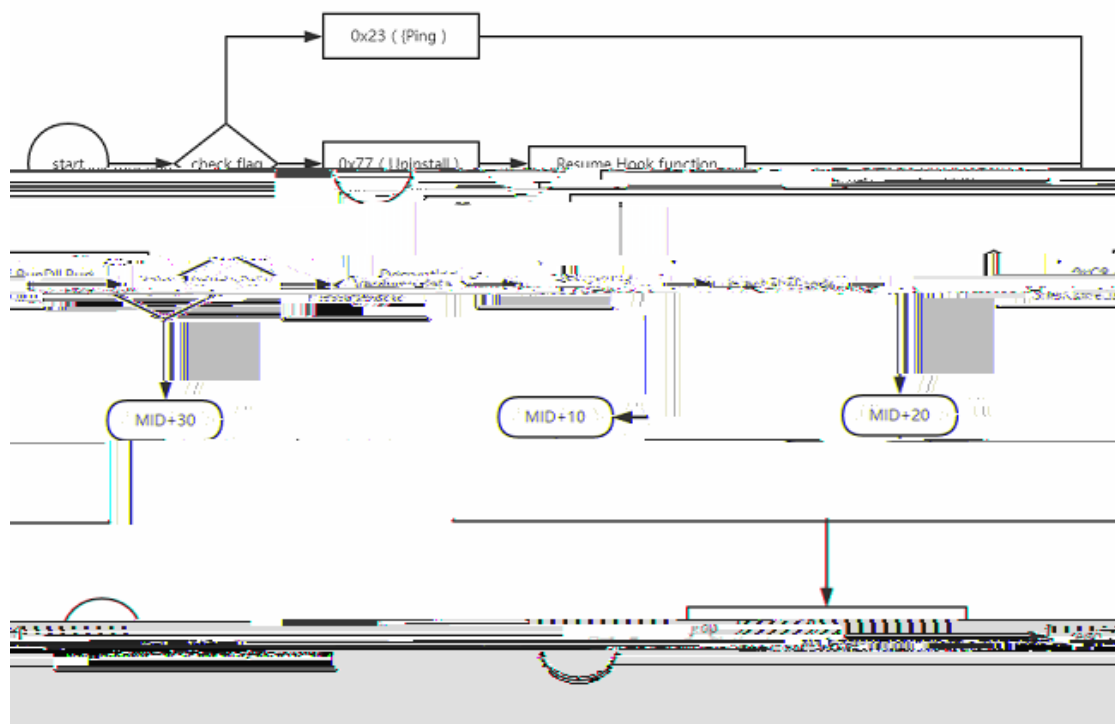


3.DoublePulsar

OutputInstall	shellcode RunShellcode
Ping	DoublePulsar
RunDLL RunShellcode	shellcode Dll



(1)CheckFlag

SMB_COM_TRANSACTION2

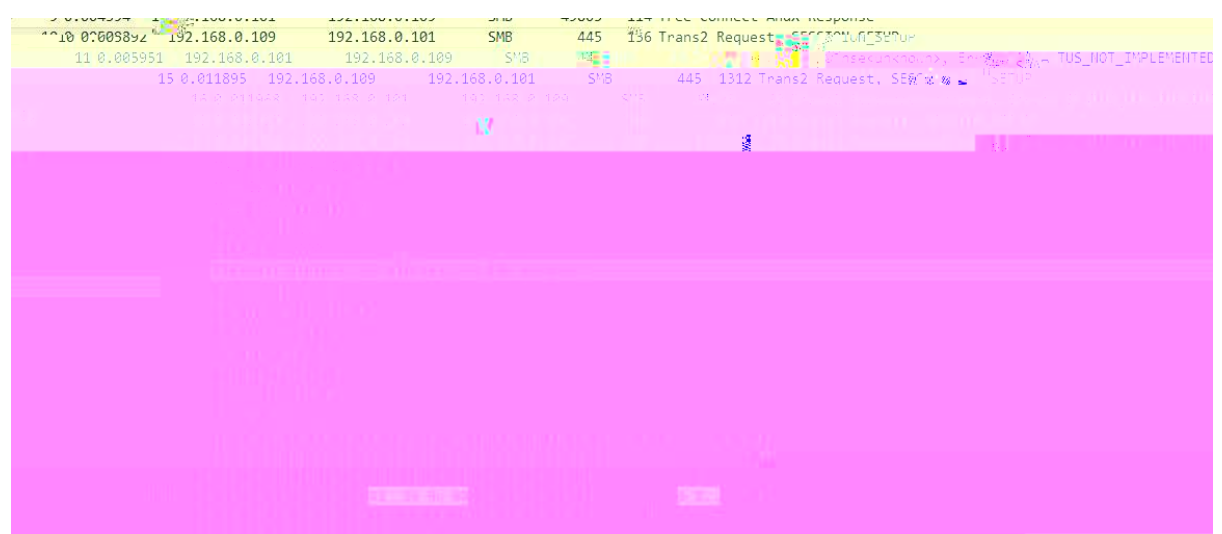
```

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



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
seg000:866F935B      call     dword ptr [edi+24h] ; PsSetProcessImageFileName

```

[illegible]

(4)Uninstall

SrvTransaction2DispatchTable

(5)

SrvTransactionNotImplemented

MID

```

Seg000:86847140
Seg000:86847140 loc_86847140: ; CODE XREF: start+54fj
-----86847140
Seg000:86847140
Seg000:86847142
Seg000:86847144 ; -----
1fj Seg000:86847144 loc_86847144: ; CODE XREF: start+4
Seg000:86847144 ; start+7Ffj ...
Seg000:86847144 mov al, 20h ; ' '
Seg000:86847146 jmp short loc_8684714C
-----
Bfj Seg000:86847148 loc_86847148: ; CODE XREF: start+9
Seg000:86847148 mov al, 30h ; '0'
Seg000:8684714A jmp short $+2
-----
Afj Seg000:8684714C loc_8684714C: ; CODE XREF: start+F
Seg000:8684714C ; start+FEfj ...
Seg000:8684714E mov ecx, [ebp+38h]
Seg000:86847150 mov ah, 0
Seg000:86847152 add [ecx+1Eh], ax , add new
-----
4fj Seg000:86847155 loc_86847155: ; CODE XREF: start+2
Seg000:86847155 mov eax, [ebp+10h]
Seg000:86847158 mov [esp+20h+var_4], eax
Seg000:8684715C popa
Seg000:8684715E jmp dword ptr [eax+3Ch] ; jmp old_SrvTra
-----
nsactionNotImplemented
Seg000:86847160

```

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



VenusEye

VenusEye

Hedwig

Locky

18

Sage 2.0

Office

0day

2016

