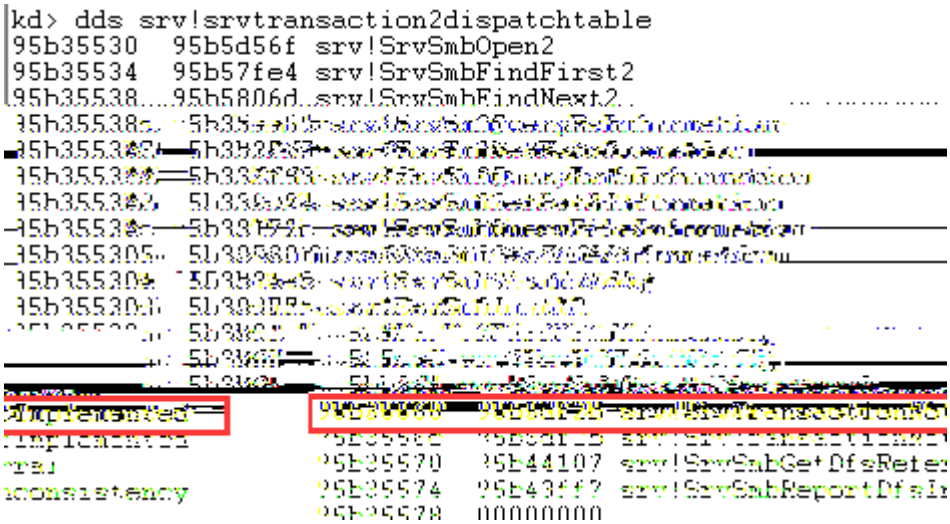
Shadow Brokers NSA DoublePulsar
DoublePulsar

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

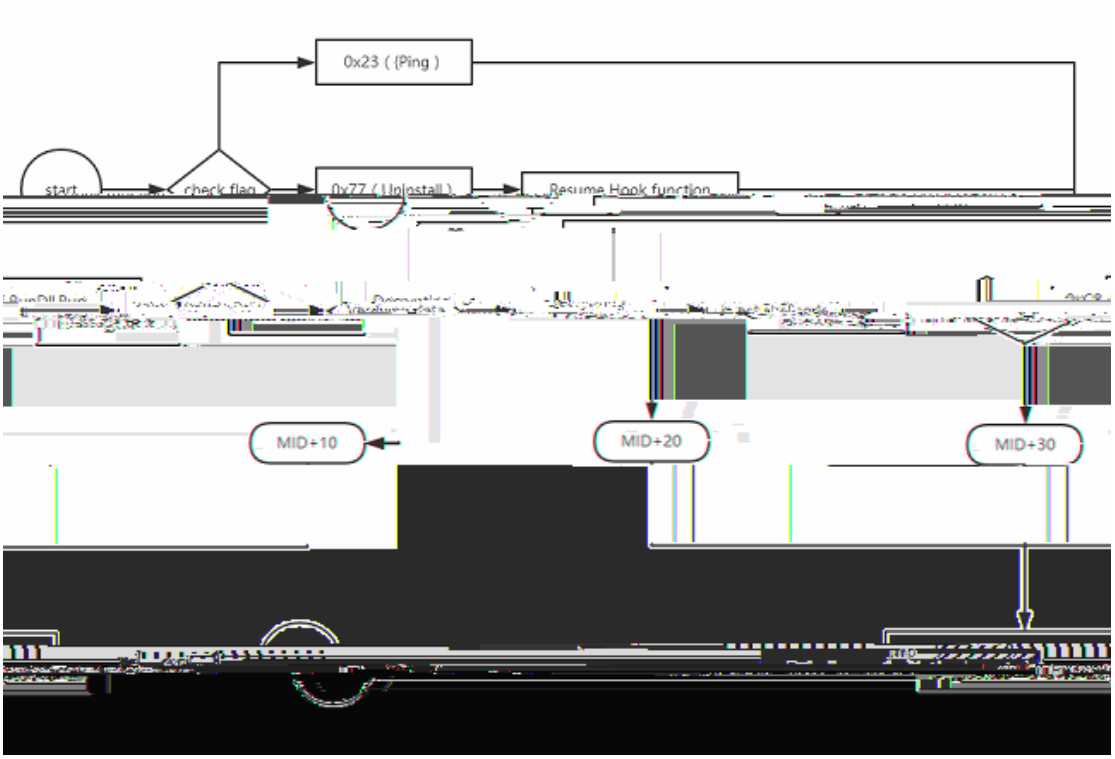
1. SrvTransaction2DispatchTable 14
SrvTransactionNotImplemented



2. SrvTransaction2DispatchTable 14

3.DoublePulsar

OutputInstall	shellcode RunShellcode
Ping	DoublePulsar
RunDLL RunShellcode	shellcode Dll



(1)CheckFlag

SMB_COM_TRANSACTION2

Timeout flag

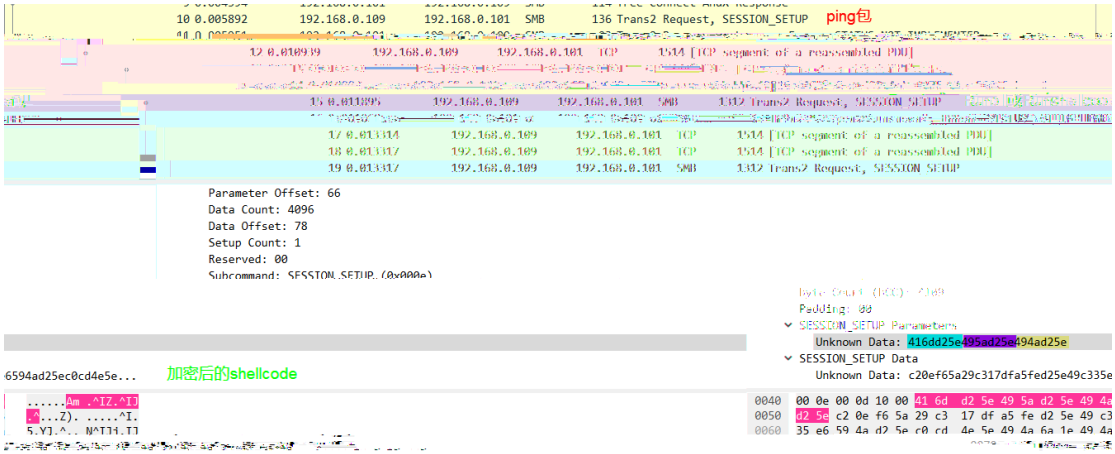
```
seg000:86847194 sub_86847194    proc near               ; CODE XREF: start+30↑p
seg000:86847194                 xor     eax, eax
seg000:86847196                 mov     al, cl
seg000:86847198                 shr     ecx, 8
seg000:8684719B                 add     al, cl
seg000:8684719D                 shr     ecx, 8
seg000:868471A0                 add     al, cl
                                sub_86847194    endp
seg000:868471A7
```

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      4805   93 Trans2 Response<unknown>, Error: STATUS_NOT_IMPLEMENTED
 15 0.011895   192.168.0.109   192.168.0.101   SMB      445   1312 Trans2 Request, SESSION_SETUP
 16 0.011968   192.168.0.101   192.168.0.109   SMB      4805   93 Trans2 Response<unknown>, Error: STATUS_NOT_IMPLEMENTED
 19 0.013317   192.168.0.109   192.168.0.101   SMB      445   1312 Trans2 Request, SESSION_SETUP
 21 0.013726   192.168.0.101   192.168.0.109   SMB      4805   93 Trans2 Response<unknown>, Error: STATUS_NOT_IMPLEMENTED
    Max Parameter Count: 1
    Max Data Count: 0
    Max Setup Count: 0
    Reserved: 00
    Flags: 0x0000
```

0x23	Ping
0x77	
0xc8	shellcode

(



SESSION_SETUP Data shellcode

a. shellcode

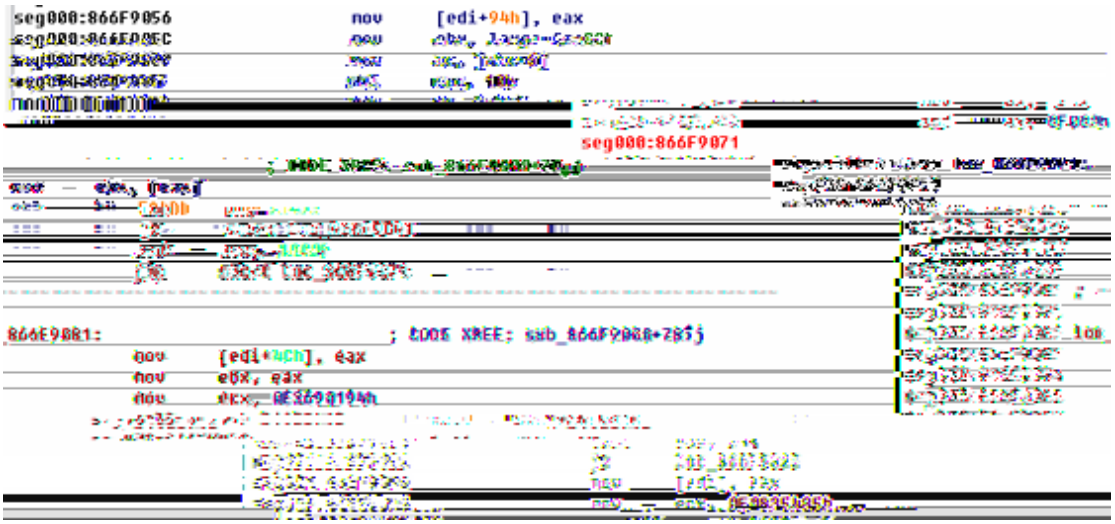
```
seg000:868470B1                 mov     esi, [eax]      ; shellcode size
seg000:868470B3                 xor     esi, [ebp+28h]  ; key
seg000:868470B6                 mov     edi, [eax+8]
seg000:868470B9                 xor     edi, [ebp+28h]
seg000:868470BC                 mov     eax, [eax+4]
seg000:868470BF                 xor     eax, [ebp+28h]
                                cmp     eax, [edx+14h]
```

b. shellcode shellcode

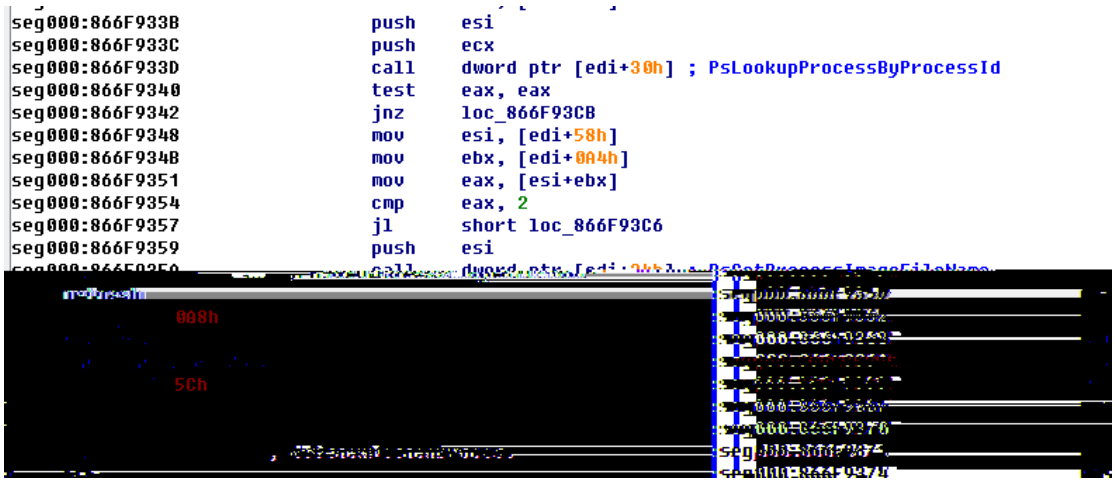
shellcode

```
seg000:868470CE                 mov     eax, [ebp+2Ch]
                                push    0               ; flProtect
                                push    1000h           ; flAllocationType
                                push    esi             ; dwSize
                                push    0               ; lpAddress
                                call    VirtualAlloc    ; Allocate buffer
                                mov     ebx, eax
                                mov     edx, [ebp+2Ch]
                                mov     esi, [edx+3Ch]
                                add     esi, edx
                                mov     esi, [esi+28h]
                                add     esi, edx
                                mov     edx, [ebp+2Ch]
                                mov     eax, [edx+30h]
                                add     esi, eax
                                mov     eax, [ebp+2Ch]
                                mov     edx, [eax+3Ch]
                                add     edx, eax
                                mov     edx, [edx+28h]
                                add     edx, eax
                                mov     eax, [ebp+2Ch]
                                mov     eax, [eax+30h]
                                add     eax, [ebp+2Ch]
                                mov     ecx, [ebp+2Ch]
                                mov     ecx, [ecx+3Ch]
                                add     ecx, [ebp+2Ch]
                                mov     ecx, [ecx+2Ch]
                                add     ecx, [ebp+2Ch]
                                mov     [ebp+3Ch], ecx
                                mov     ecx, [ebp+2Ch]
                                mov     ecx, [ecx+3Ch]
                                add     ecx, [ebp+2Ch]
                                mov     ecx, [ecx+28h]
                                add     ecx, [ebp+2Ch]
                                mov     [ebp+28h], ecx
loc_8684710B:                                           ; CODE XREF: start+C8↓j
                                xor     [esi], ebx
                                add     esi, 4
                                loop    loc_8684710B    ; decrpyt data
                                add     eax, edx
                                cmp     esi, eax
                                jl      short loc_86847140
                                mov     eax, [ebp+2Ch]
                                pusha
                                mov     esi, esp
                                push    eax
                                call    eax
                                mov     esp, esi
```

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



d. PID lsass.exe



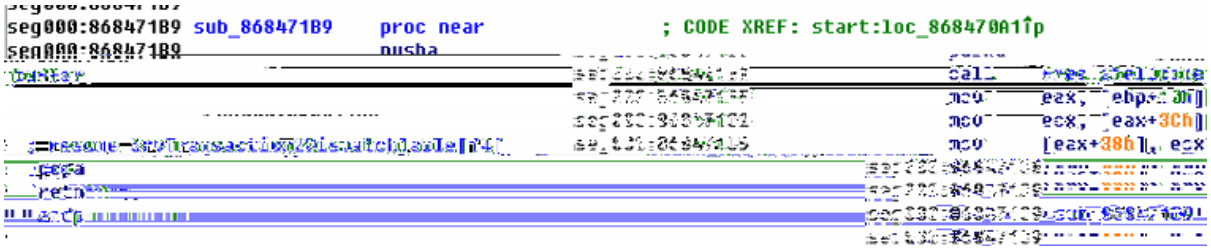
e. APC



(4)Uninstall

0x77

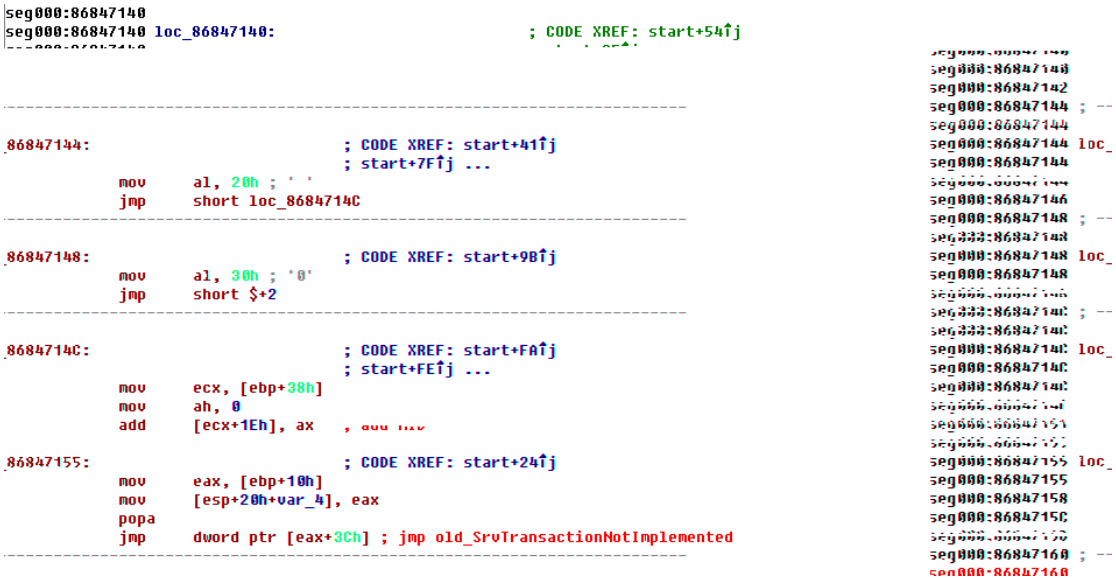
SrvTransaction2DispatchTable



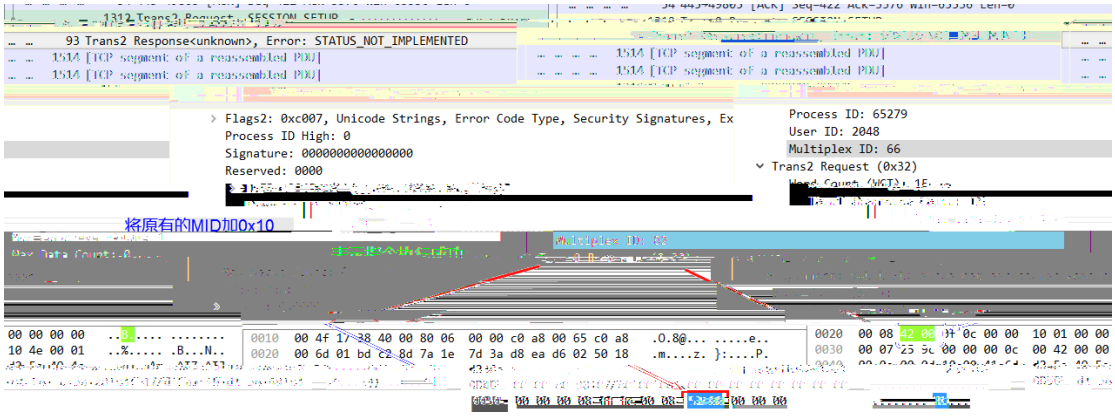
(5)

SrvTransactionNotImplemented

MID



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



VenusEye

VenusEye

Hedwig Locky

18

Sage 2.0

Office 0day 2016



