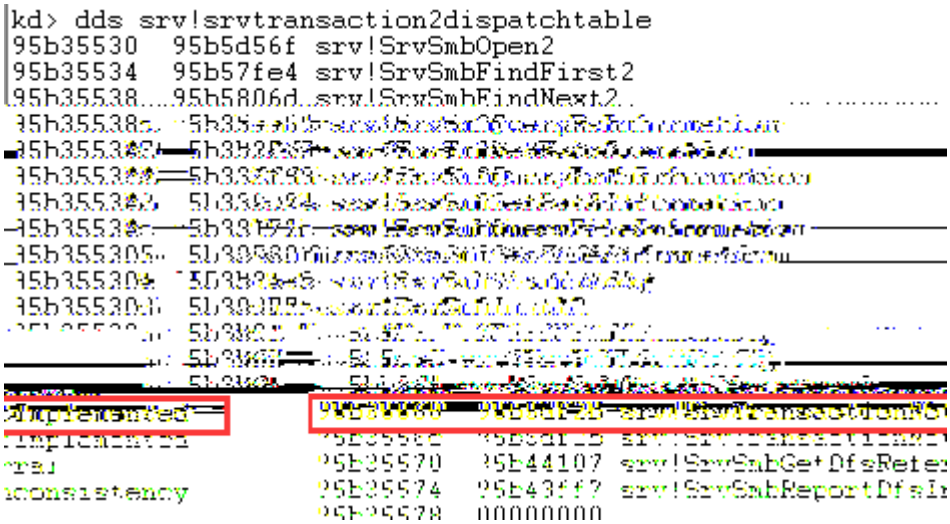
Shadow Brokers NSA DoublePulsar
DoublePulsar

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

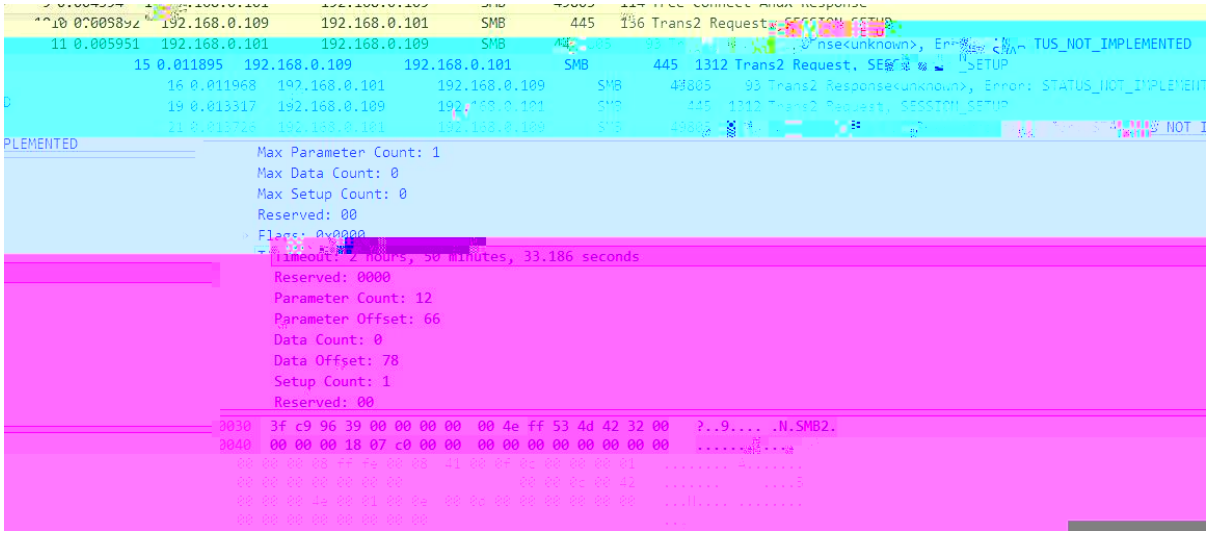
(1)CheckFlag

SMB_COM_TRANSACTION2

Timeout flag

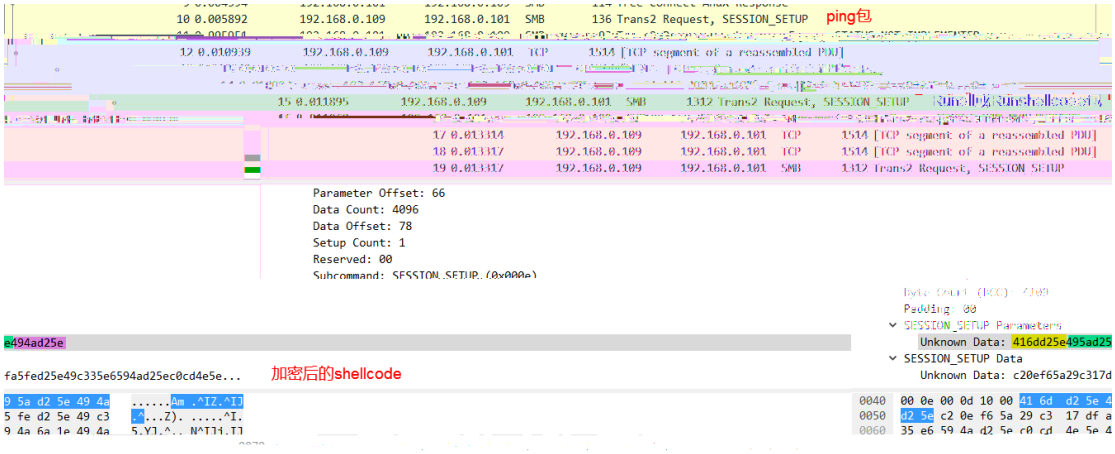
```
seg000:86847194 sub_86847194    proc near               ; CODE XREF: start+30↑p
seg000:86847194                 xor     eax, eax
seg000:86847196                 mov     al, cl
seg000:86847198                 shr     ecx, 8
seg000:8684719B                 add     al, cl
seg000:8684719D           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

timeout 0x23



0x23	Ping
0x77	
0xc8	shellcode

(



SESSION_SETUP Data shellcode

a. shellcode

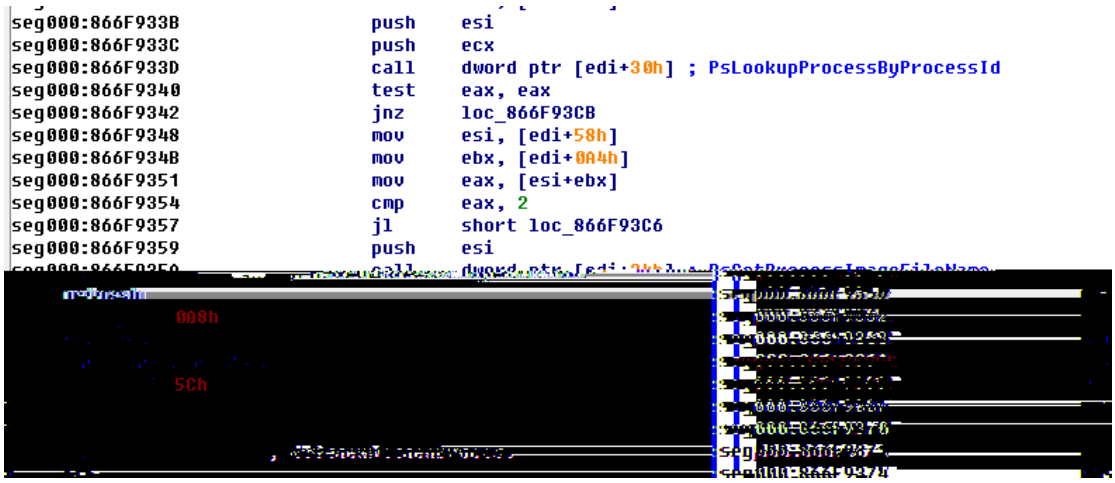
```
seg000:868470B1        mov     esi, [eax]      ; shellcode size
seg000:868470B3        xor     esi, [ebp+28h]  ; key
seg000:868470B6        mov     edi, [eax+8]
seg000:868470B9        xor     edi, [ebp+28h]
seg000:868470BC        mov     eax, [eax+4]
seg000:868470BF        xor     eax, [ebp+28h]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

b. shellcode shellcode

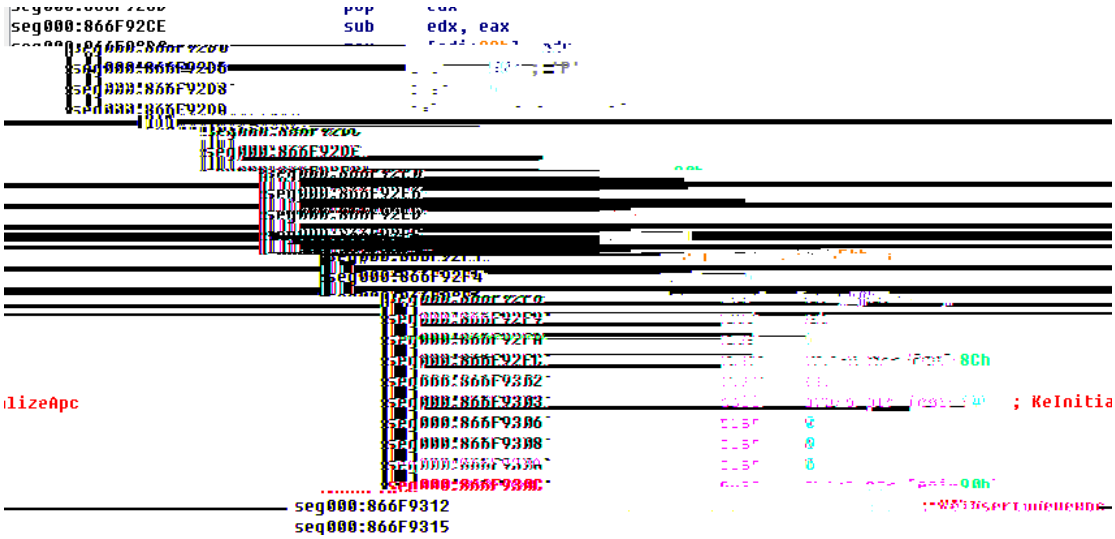
shellcode

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

d. PID lsass.exe



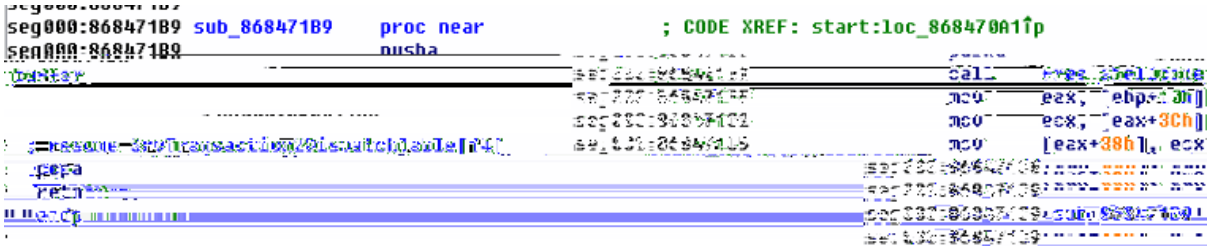
e. APC



(4)Uninstall

0x77

SrvTransaction2DispatchTable



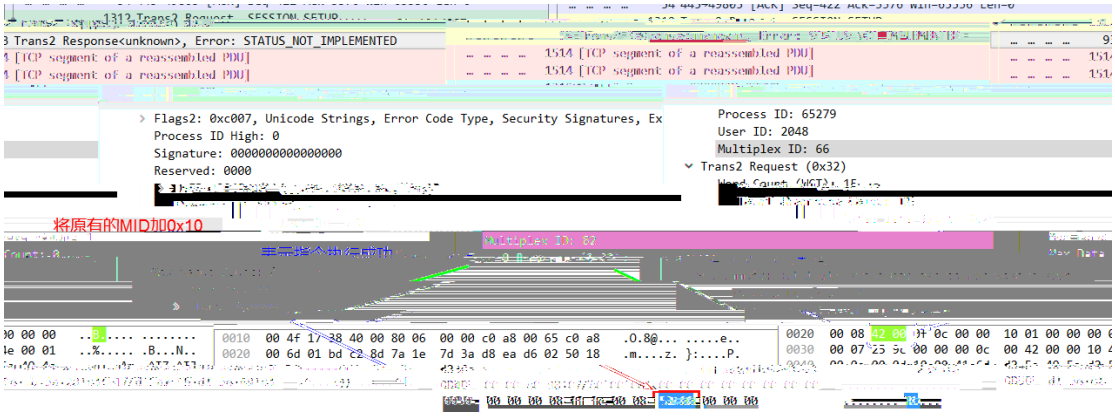
(5)

SrvTransactionNotImplemented

MID

```
seg000:86847140
seg000:86847140 loc_86847140:                           ; CODE XREF: start+54↑j
86847140
86847142
86847144 ; ---------------------------------------------------------------------------
86847144
86847144 loc_86847144:                                  ; CODE XREF: start+41↑j
86847144                                                ; start+7F↑j ...
                mov     al, 20h ; ' '
86847146        jmp     short loc_8684714C
86847148 ; ---------------------------------------------------------------------------
86847148
86847148 loc_86847148:                                  ; CODE XREF: start+9B↑j
86847148        mov     al, 30h ; '0'
                jmp     short $+2
8684714C ; ---------------------------------------------------------------------------
8684714C
8684714C loc_8684714C:                                  ; CODE XREF: start+FA↑j
8684714C                                                ; start+FE↑j ...
8684714C        mov     ecx, [ebp+38h]
                mov     ah, 0
                add     [ecx+1Eh], ax
86847155 loc_86847155:                                  ; CODE XREF: start+24↑j
86847155        mov     eax, [ebp+10h]
86847158        mov     [esp+20h+var_4], eax
8684715C        popa
                jmp     dword ptr [eax+3Ch] ; jmp old_SrvTransactionNotImplemented
86847160 ; ---------------------------------------------------------------------------
```

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

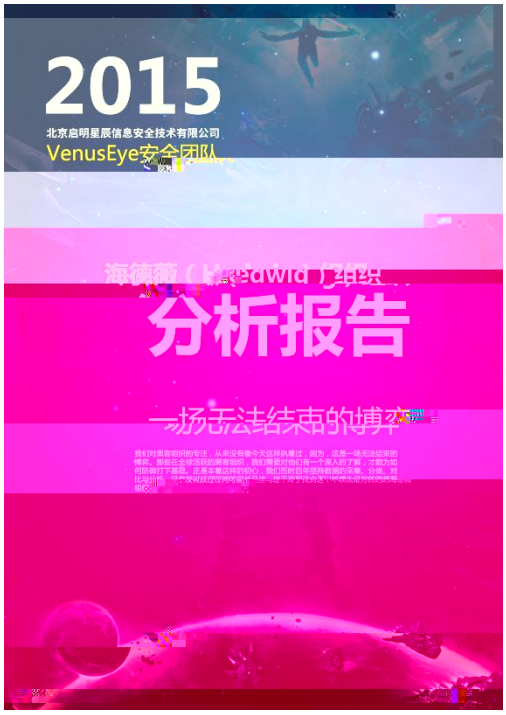


VenusEye

VenusEye

Hedwig Locky

18

Sage 2.0

Office 0day 2016