

Attack
Time
Window

(Thread 0)

...

mov [eax+var_48], eax

mov ebx, [eax+4]

add ebx, 0Ch

mov ebx, [ebp+var_24], ebx

test ebx, ebx

jnz bailout

push 1

push 63737355h

push ebx

call

UserAllocPoolWithQuota

...

mov [eax+8], edi

mov eax, ecx

mov ecx, [eax+4]

mov esi, [eax+8]

mov eax, ecx

shr ecx, 2

rep movsd

(Thread 1)

mov eax, pcbData

...

...

...

xor [eax], 0x80000

xor [eax], 0x80000

xor [eax], 0x80000

xor [eax], 0x80000

xor [eax], 0x80000

xor [eax], 0x80000

xor [eax], 0x80000

xor [eax], 0x80000

xor [eax], 0x80000

xor [eax], 0x80000

...

...

...

