

(Thread 0 -> syscall)

...

...

cmp [eax+8], ebx ; ① eax=0x0

...

mov ebx, [eax+4] ; ② eax=0x0

add ebx, 0Ch

...

call UserAllocPoolWithQuota

...

mov ecx, [eax+4] ; ③ eax=0x0

mov esi, [eax+8]

mov eax, ecx

shr ecx, 2

rep movsd

...

(syscall ends)

...

...

Attack
Time
Window

Page
Protect
Window

(Thread 1 attack)

...

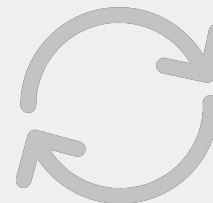
mov eax, 0x4

xor [eax], 0x80000



(Page fault enter)

Write Conflict
Sleep()



Check()
(Page fault return)

xor [eax], 0x80000