The new function is the same in winresume. There are some differences in the calling. Green highlight is parts that are different from winload.

Original code (total 25 bytes):

.text:004028AC mov eax, graphics\_pack ; A1 ?? ?? 48 00

.text:004028B1 mov ecx, [eax] ; 8B 08

.text:004028B3 test ecx, ecx ; 85 C9

.text:004028B5 jz short loc\_4028C5 ; 74 0E

.text:004028B7 add eax, 8 ; 83 C0 08

.text:004028BA push eax ; 50

.text:004028BB push ecx ; 51

.text:004028BC call \_BgpGxDrawBitmapImage@12 ; E8 ?? ?? 03 00

.text:004028C1 test eax, eax ; 85 C0

.text:004028C3 jl short loc\_4028CA ; 7C 05

New Code (total 9 bytes):

.text:004028AC call \_TheNewFunction@0 ; E8 [XX XX XX XX] (relative)

.text:004028B1 test eax, eax ; 85 C0 (if eax>=0, jump)

.text:004028B3 jge/jnl short loc\_4028D0 ; 7D [1B] (relative)

(jumps over BgpDrawCopyright and BgDisplayString)

.text:004028B5 through .text:4028C5 are 16 nops (90)

Relocation removal:

Zero out:

.reloc / IMAGE\_DIRECTORY\_ENTRY\_BASERELOC : RVA 2000 : 38AD

The image is stored in “wimresume.exe : RC\_DATA : 1”