

```

sub_409B78 proc near
f1NewProtect= dword ptr -54h
SystemInfo= _SYSTEM_INFO ptr -50h
Buffers _MEMORY_BASIC_INFORMATION ptr -2Ch
    push    ebx
    push    esi
    push    edi
    push    ebp
    add     esp, OFFFFFFFBCh
    mov     edi, eax
    lea     eax, [esp+54h+Buffer]
    lea     eax, [esp+54h+SystemInfo]
    push    eax          ; lpSystemInfo
    call    GetSystemInfo
    mov     eax, edi
    push    1Ch           ; dwLength
    push    esi           ; lpBuffer
    push    ebx           ; lpAddress
    call    VirtualQuery
    test   eax, eax
    jz     loc_409C2C

```

```

    jmp    short loc_409C21

```

```

loc_409C21:
    mov     eax, [esi+4]
    cmp     eax, edi
    jz     loc_409BA4

```

```

loc_409BA4:
    cmp     dword ptr [esi+10h], 1000h
    jnz    short loc_409COD

```

```

test   byte ptr [esi+15h], 1
jnz    short loc_409COD

```

```

xor    ebx, ebx
mov    eax, [esi+14h]
cmp    eax, 1
jz     short loc_409BCC

```

```

cmp    eax, 2
jz     short loc_409BCC

```

```

cmp    eax, 10h
jz     short loc_409BCC

```

```

cmp    eax, 20h
jnz    short loc_409BE1

```

```

loc_409BCC:      ; lpf1OldProtect
    push    esp
    push    40h          ; f1NewProtect
    mov     eax, [esi+0Ch]
    push    eax          ; dwSize
    mov     eax, [esi]
    push    eax          ; lpAddress
    call    VirtualProtect
    test   eax, eax
    jz     short loc_409BE1

```

```

    mov    bl, 1

```

```

loc_409BE1:
    xor    ebp, ebp
    jmp    short loc_409BF2

```

```

loc_409BF2:
    cmp    ebp, [esi+0Ch]
    jb     short loc_409BE5

```

```

loc_409BE5:
    mov    eax, [esi]
    add    eax, ebp
    call    sub_409B70
    add    ebp, [esp+54h+SystemInfo.dwPageSize]

```

```

push    esp          ; lpf1OldProtect
mov    eax, [esp+58h+f1NewProtect]
push    eax          ; f1NewProtect
mov    eax, [esi+0Ch] ; dwSize
push    eax          ; lpAddress
call    VirtualProtect

```

```

loc_409COD:
    mov    eax, [esi]
    add    eax, [esi+0Ch]
    mov    ebx, eax
    push    1Ch           ; dwLength
    push    esi           ; lpBuffer
    push    ebx           ; lpAddress
    call    VirtualQuery
    test   eax, eax
    jz     short loc_409C2C

```

```

loc_409C2C:
    add    esp, 44h
    pop    ebp
    pop    edi
    pop    esi
    pop    ebx
    ret
sub_409B78 endp

```