

Re: Interesting Web Site on Open Source Development

Source: <http://coding.derkeiler.com/Archive/Assembler/alt.lang.asm/2005-04/msg01047.html>

- *From:* "o/annabee" <<http://www.TheWannabee.Org>>
 - *Date:* Fri, 22 Apr 2005 23:24:52 +0200
-

På Fri, 22 Apr 2005 22:24:20 +0200, skrev f0dder <f0dder@xxxxxxxxxxxxxxxxxxxx>:

:))

```
Code0401000: A0:
    sub esp 090
    mov D$esp+04 0BADCODE
    mov D$esp 0DEADBEEF
    call Code04013A0
    test al al | jne I7> ; Code0401057
    call Code0401100
    push eax
    lea eax D$esp+014
    push Data0402124
    push eax
    call 'USER32.wsprintfA'
    add esp 0C
    push 030
    lea ecx D$esp+014
    push ecx
    push Data04020F8
    push 00
    call 'USER32.MessageBoxA'
    mov eax 01
    add esp 090
    ret
```

```
Code0401057: I7:
    push esi
    rdtsc
    mov D$esp+010 edx
    mov D$esp+0C eax
```

Re: Interesting Web Site on Open Source Development

```
lea edx D$esp+04
push edx
lea eax D$esp+0C
push eax
push 010
call Code0401110
test al al
mov esi 'USER32.MessageBoxA' | jne 01> ; Code040108D
push 030
push Data04020F0
push Data04020D0
push 00
call esi
```

```
Code040108D: 01:
call Code04013D0
test al al | jne A6> ; Code04010A6
push 030
push Data04020F0
push Data04020A4
push 00
call esi
```

```
Code04010A6: A6:
mov eax D$esp+04
mov ecx D$esp+0C
mov edx eax
sub edx ecx
push edx
mov edx D$esp+0C
push ecx
mov ecx D$esp+018
push ecx
push eax
push edx
lea eax D$esp+028
push Data0402070
push eax
call 'USER32.wsprintfA'
add esp 01C
push 00
push Data0402050
lea ecx D$esp+01C
push ecx
push 00
call esi
xor eax eax
pop esi
add esp 090
ret
```

Align 04

Re: Interesting Web Site on Open Source Development

Main:

```
Code04010F0: I0:
    call Code0401000
    push eax
    call 'KERNEL32.ExitProcess'
    Align 04
```

```
Code0401100: J6:
    mov eax D$Data0403030
    ret
```

Align 010

```
Code0401110: L2:
    mov al B$Data040302C
    sub esp 08
    test al al | je F9> ; Code040117B
    mov eax D$esp+0C
    push 00
    lea ecx D$esp+010
    push ecx
    mov ecx D$Data040303C
    push 08
    lea edx D$esp+0C
    push edx
    push 04
    mov D$esp+014 eax
    mov eax edx
    push eax
    push 022E000
    push ecx
    call 'KERNEL32.DeviceIoControl'
    test eax eax | jne D2> ; Code0401160
    call 'KERNEL32.GetLastError'
    mov D$Data0403030 eax
    xor al al
    add esp 08
    ret 0C
```

```
Code0401160: D2:
    mov edx D$esp+010
    mov eax D$esp
    mov ecx D$esp+014
    mov D$edx eax
    mov edx D$esp+04
    mov D$ecx edx
    mov al 01
    add esp 08
    ret 0C
```

Re: Interesting Web Site on Open Source Development

Code040117B: F9:

```
mov eax D$esp+014
mov ecx D$esp+010
mov edx D$esp+0C
push eax
push ecx
push edx
call Code040147C
mov al 01
add esp 08
ret 0C
```

Code0401220: G4:

```
mov eax D$Data0403034
test eax eax
push esi
mov esi D$Data0403010
push edi
mov edi D$Data0403024 | je K8> ; Code040124C
push eax
call esi
mov eax D$Data0403034
push eax
call edi
mov D$Data0403034 0
```

Code040124C: K8:

```
mov eax D$Data0403038
test eax eax | je N9> ; Code040126B
push eax
call esi
mov ecx D$Data0403038
push ecx
call edi
mov D$Data0403034 0
```

Code040126B: N9:

```
pop edi
pop esi
ret
```

Align 04

Code0401270: 04:

Re: Interesting Web Site on Open Source Development

```
sub esp 0108
push 0F003F
push 00
push 00
call D$Data040301C
test eax eax
mov D$Data0403034 eax | jne D4> ; Code04012A2
call 'KERNEL32.GetLastError'
mov D$Data0403030 eax
xor al al
add esp 0108
ret
```

Code04012A2: D4:

```
lea eax D$esp
push eax
push 0105
call 'KERNEL32.GetCurrentDirectoryA'
mov ecx D$Data0403000
push ecx
lea edx D$esp+04
push edx
call 'KERNEL32.lstrcatA'
mov ecx D$Data0403000
push 00
mov edx D$Data0403034
push 00
push 00
push 00
push 00
lea eax D$esp+014
push eax
push 00
push 03
push 01
push 0F01FF
push Data0402154
inc ecx
push ecx
push edx
call D$Data0403018
test eax eax
mov D$Data0403038 eax | je C0> ; Code0401334
push 00
push 00
push eax
call D$Data0403014
test eax eax | je C0> ; Code0401334
mov eax D$Data0403004
push 00
push 00
push 03
push 00
push 03
push 0C0000000
push eax
call 'KERNEL32.CreateFileA'
cmp eax 0-01
mov D$Data040303C eax | jne E5> ; Code040134D
```

Re: Interesting Web Site on Open Source Development

```
Code0401334: C0:
    call 'KERNEL32.GetLastError'
    mov D$Data0403030 eax
    call Code0401220
    xor al al
    add esp 0108
    ret
```

```
Code040134D: E5:
    mov al 01
    add esp 0108
    ret
```

```
Code04013A0: M8:
    call 'KERNEL32.GetVersion'
    shr eax 01F
    not al
    and al 01
    mov B$Data040302C al | je P9> ; Code04013BF
    call Code0401270
    mov B$Data040302D al
    ret
```

```
Code04013BF: P9:
    mov al 01
    mov B$Data040302D al
    ret
```

Align 010

```
Code04013D0: B6:
    mov cl B$Data040302C
    xor al al
    sub esp 01C
    cmp cl al
    mov B$Data040302D al | je K2> ; Code0401426
    mov eax D$Data040303C
    push ebx
    push eax
    call 'KERNEL32.CloseHandle'
    mov edx D$Data0403038
    lea ecx D$esp+04
    push ecx
```

Re: Interesting Web Site on Open Source Development

```
push 01
push edx
call D$Data0403020
test eax eax
setne bl
call Code0401220
call 'KERNEL32.GetLastError'
mov D$Data0403030 eax
call Code0401220
mov al bl
pop ebx
add esp 01C
ret
```

Code0401426: K2:

```
mov al 01
add esp 01C
ret
```

Align 04

Code0401430: L2:

```
push ebp
mov ebp esp
add esp 0-08
push esi
sibt X$ebp-06
mov esi D$ebp-04
push D$esi+028
push D$esi+02C
push D$ebp+08
pop W$esi+028
pop W$esi+02E
int 05
pop D$esi+02C
pop D$esi+028
pop esi
leave
ret 04
```

Code0401462: A2:

```
push ebp
mov ebp esp
mov ecx D$ebp+08
mov edx D$ebp+0C
mov eax D$ebp+010
push Data040145F
call Code0401430
leave
ret 0C
```

Re: Interesting Web Site on Open Source Development

Code040147C: C8:

```
push ebp
mov ebp esp
mov ecx D$ebp+08
push Data040145C
call Code0401430
mov ecx D$ebp+0C
mov D$ecx edx
mov ecx D$ebp+010
mov D$ecx eax
leave
ret 0C
```

Code040149A: F8:

```
mov eax Data0403024
jmp Code04014A4
```

Code04014A4: G8:

```
push ecx
push edx
push eax
push Data0402180
call Code04014E7
pop edx
pop ecx
jmp eax
```

Code04014B5: I5:

```
mov eax Data0403010
jmp Code04014A4
```

Code04014BF: J5:

```
mov eax Data0403014
jmp Code04014A4
```

Code04014C9: K5:

```
mov eax Data0403018
jmp Code04014A4
```

Code04014D3: L5:

```
mov eax Data040301C
jmp Code04014A4
```

Re: Interesting Web Site on Open Source Development

Code04014DD: M5:

```
    mov eax Data0403020
    jmp Code04014A4
```

Code04014E7: N5:

```
    push ebp
    mov ebp esp
    sub esp 044
    push ebx
    mov eax 0400000
    push esi
    mov esi D$ebp+08
    mov edx D$esi+08
    mov ecx D$esi+04
    mov ebx D$esi+0C
    add edx eax
    push edi
    mov edi D$esi+014
    add edi eax
    add ecx eax
    mov D$ebp-018 edx
    mov edx D$esi+010
    add ebx eax
    add edx eax
    mov eax D$esi+01C
    mov D$ebp-04 eax
    mov eax D$ebp+0C
    mov D$ebp-038 ecx
    xor ecx ecx
    mov D$ebp-0C edi
    mov D$ebp-03C eax
    xor eax eax
    test D$esi 01
    lea edi D$ebp-030
    mov D$ebp-044 024
    mov D$ebp-040 esi
    mov D$ebp-034 ecx
    stosd
    mov D$ebp-02C ecx
    mov D$ebp-028 ecx
    mov D$ebp-024 ecx | jne K7> ; Code040156B
    lea eax D$ebp-044
    mov D$ebp+0C eax
    lea eax D$ebp+0C
    push eax
    push 01
    push ecx
    push 0C06D0057
    call 'KERNEL32.RaiseException'
    xor eax eax
    jmp Code0401723
```

Code040156B: K7:

```
    mov eax D$ebp-018
```

Re: Interesting Web Site on Open Source Development

```
mov edi D$eax
mov eax D$ebp+0C
sub eax ebx
sar eax 02
shl eax 02
add edx eax
mov edx D$edx
mov D$ebp+08 eax
mov eax edx
shr eax 01F
not eax
and eax 01
mov D$ebp-034 eax | je P6> ; Code040159C
lea eax D$edx+
mov D$ebp-030 eax
jmp A5> ; Code04015A5
```

```
Code040159C: P6:
and edx 0FFFF
mov D$ebp-030 edx
```

```
Code04015A5: A5:
mov eax D$Data040304C
xor ebx ebx
cmp eax ecx | je D3> ; Code04015C1
lea edx D$ebp-044
push edx
push ecx
call eax
mov ebx eax
test ebx ebx | jne Code0401706
```

```
Code04015C1: D3:
test edi edi | jne Code040166B
mov eax D$Data040304C
test eax eax | je G4> ; Code04015E0
lea ecx D$ebp-044
push ecx
push 01
call eax
mov edi eax
test edi edi | jne 04> ; Code0401630
```

```
Code04015E0: G4:
push D$ebp-038
call 'KERNEL32.LoadLibraryA'
mov edi eax
test edi edi | jne 04> ; Code0401630
call 'KERNEL32.GetLastError'
mov D$ebp-024 eax
mov eax D$Data0403048
test eax eax | je L1> ; Code040160F
```

Re: Interesting Web Site on Open Source Development

```
lea ecx D$ebp-044
push ecx
push 03
call eax
mov edi eax
test edi edi | jne 04> ; Code0401630
```

```
Code040160F: L1:
lea eax D$ebp-044
mov D$ebp+0C eax
lea eax D$ebp+0C
push eax
push 01
push 00
push 0C06D007E
call 'KERNEL32.RaiseException'
mov eax D$ebp-028
jmp Code0401723
```

```
Code0401630: 04:
push edi
push D$ebp-018
call 'KERNEL32.InterlockedExchange'
cmp eax edi | je D6> ; Code0401664
cmp D$esi+018 00 | je E3> ; Code040166B
push 08
push 040
call 'KERNEL32.LocalAlloc'
test eax eax | je E3> ; Code040166B
mov D$eax+04 esi
mov ecx D$Data0403044
mov D$eax ecx
mov D$Data0403044 eax
jmp E3> ; Code040166B
```

```
Code0401664: D6:
push edi
call 'KERNEL32.FreeLibrary'
```

```
Code040166B: E3:
mov eax D$Data040304C
test eax eax
mov D$ebp-02C edi | je G5> ; Code0401681
lea ecx D$ebp-044
push ecx
push 02
call eax
mov ebx eax
```

Re: Interesting Web Site on Open Source Development

```
Code0401681: G5:
    test ebx ebx | jne D3> ; Code0401701
    cmp D$esi+014 ebx | je L8> ; Code04016B6
    cmp D$esi+01C ebx | je L8> ; Code04016B6
    mov eax D$edi+03C
    add eax edi
    cmp D$eax 04550 | jne L8> ; Code04016B6
    mov ecx D$ebp-04
    cmp D$eax+08 ecx | jne L8> ; Code04016B6
    cmp edi D$eax+034 | jne L8> ; Code04016B6
    mov eax D$ebp-0C
    mov ecx D$ebp+08
    mov ebx D$ecx+eax
    test ebx ebx | jne D3> ; Code0401701
```

```
Code04016B6: L8:
    push D$ebp-030
    push edi
    call 'KERNEL32.GetProcAddress'
    mov ebx eax
    test ebx ebx | jne D3> ; Code0401701
    call 'KERNEL32.GetLastError'
    mov D$ebp-024 eax
    mov eax D$Data0403048
    test eax eax | je A2> ; Code04016E2
    lea ecx D$ebp-044
    push ecx
    push 04
    call eax
    mov ebx eax
```

```
Code04016E2: A2:
    test ebx ebx | jne D3> ; Code0401701
    lea eax D$ebp-044
    mov D$ebp+08 eax
    lea eax D$ebp+08
    push eax
    push 01
    push ebx
    push 0C06D007F
    call 'KERNEL32.RaiseException'
    mov ebx D$ebp-028
```

```
Code0401701: D3:
    mov eax D$ebp+0C
    mov D$eax ebx
```

```
Code0401706: D8:
    mov eax D$Data040304C
    test eax eax | je G5> ; Code0401721
    and D$ebp-024 00
    lea ecx D$ebp-044
```

Re: Interesting Web Site on Open Source Development

```
push ecx
push 05
mov D$ebp-02C edi
mov D$ebp-028 ebx
call eax
```

```
Code0401721: G5:
mov eax ebx
```

```
Code0401723: G7:
pop edi
pop esi
pop ebx
leave
ret 08
```