

### Fun With Thread Local Sto

Peter Ferrie Senior Anti-virus Researcher 26 June, 2008



#### You Can Call Me Al

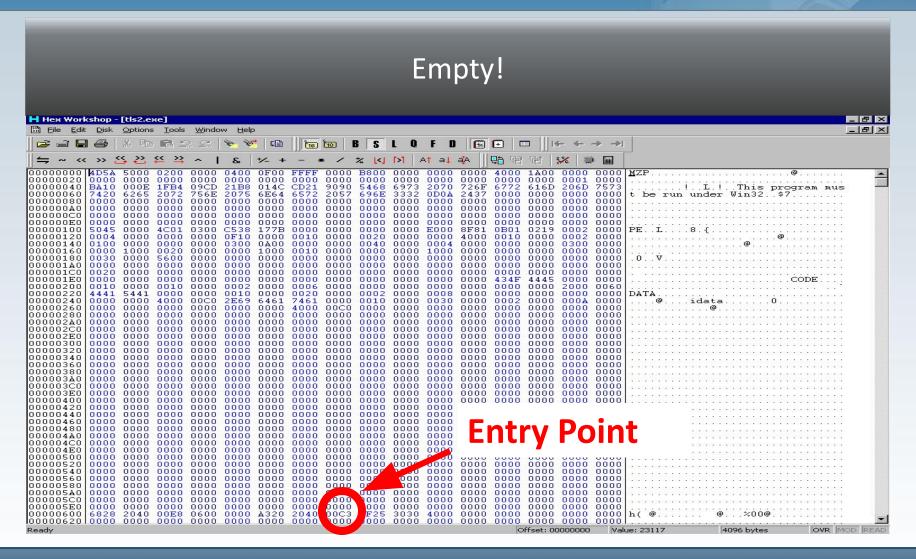
Thread Local Storage callbacks were discovered in 2000.

However, widespread use didn't occur until 2004.

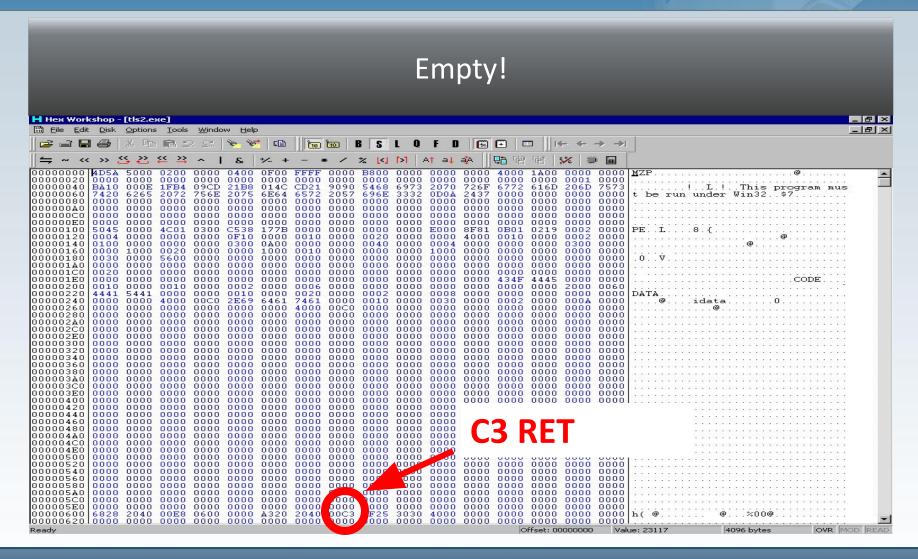
Now, it should be the first place to look for code, since it runs before the main entrypoint.

And that can make all the difference...











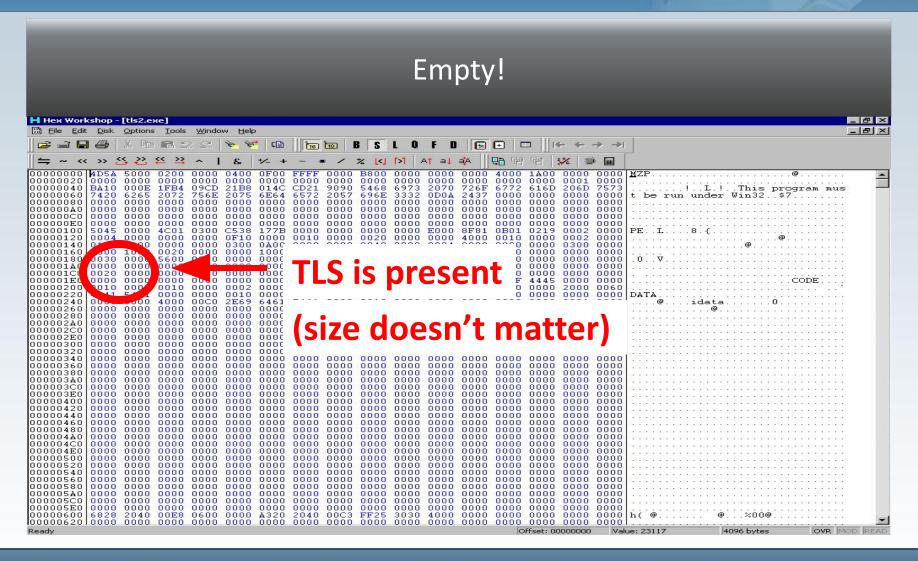
### Empty!

So the main file does nothing.

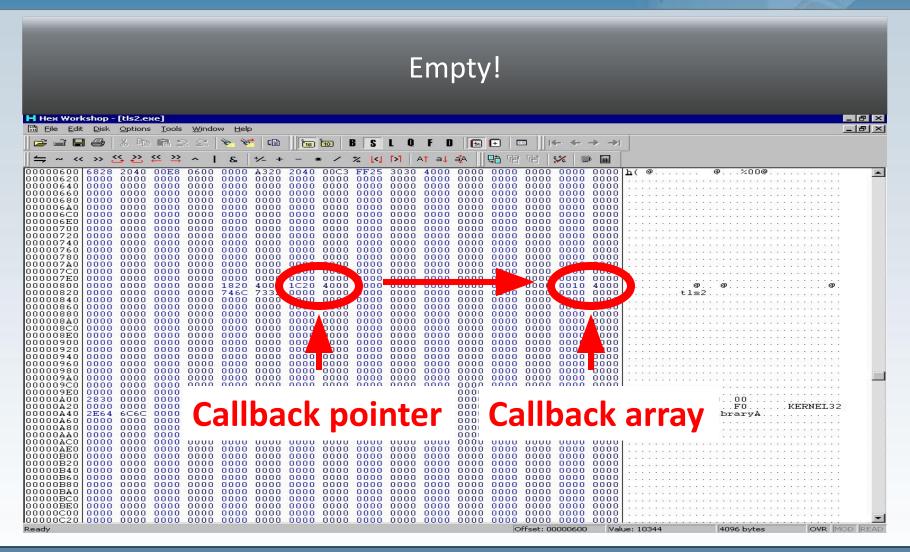
If we assume that the structure is normal,
then we could check the thread local storage table.

Just in case.











### Empty!

So the search moves to the callbacks, of which there is only one... or is there?



### The One and Only

```
ov IDA - tls2.exe
  File
                       Jump Search View
                                                        Debug
                                                                    Options Window
                                                                                                                                                                         IDA View-A
                                                   public TlsCallback 0
                                                                par ; DATA REF: HEADER:pe_headerfo ; HEADER:pe_section_tablefo ... offset LibFileName ; "tls2" j_LoadLibraryA ds:TlsCallbacksEnd, eax
                        TlsCallback 0
                                                    proc near
 CODE:00401005
                                                   call
 CODE:0040100A
CODE:0040100A
CODE:0040100A
                        TlsCallback_0 endp
 CODE:0040100F
CODE:0040100F
                                   ======= S U B R O U T I N E ====
 CODE:0040100F
 CODE:0040100F
CODE:0040100F
                                                   public start
 CODE:0040100F
                                                   proc near
 CODE: 0040100F
                                                    retn
 CODE:0040100F
                                                    endp
 CODE:0040100F
                           [00000006 BYTES: COLLAPSED FUNCTION j_LoadLibraryA. PRESS KEYPAD "+" TO EXPANDI
align 4
dd 7Ah dup(0)
dd 380h dup(?)
 CODE:00401010
 CODE:00401016
 CODE:00401018
 CODE:00401200
CODE:00401200 CODE
                                                   ends
 CODE:00401200
CODE:00401200
DATA:00402000
DATA:00402000
                           Section 2. (virtual address 00002000)
Virtual size : 00001000 (
Section size in file : 0000200 (
Offset to raw data for section: 00000800
Flags C0000040: Data Readable Writable
 DATA:00402000
DATA:00402000
 DATA:00402000
 DATA:00402000
                            Alignment
                                                   : default
 DATA:00402000
DATA:00402000
 DATA:00402000
                            Segment type: Pure data
Segment permissions: Read/Write
 DATA:00402000
                                                   segment para public 'DATA' use32
assume cs:DATA
 DATA:00402000 DATA
 DATA:00402000
DATA:00402000
                                                   TLS_DIR_ENTRY <0, 0, offset TlsIndex, offset TlsCallbacks, 0, 0>

DATA KREF: HEADER: pe_header to HEADER: 00400220 to

dd 0

dd offset TlsCallback_0; DATA KREF: DATA: TlsDirectory to

dd 0

; DATA KREF: TlsCallback_0+Atw
 DATA:00402000 TlsDirectory
 DATA:00402000
DATA:00402018
                        TlsIndex
DATA:0040201C TlsCallbacks
DATA:0040201C TlsCallbacks
DATA:00402020 TlsCallbacks
DATA:00402024
                        T1sCallbacksEnd
                                                   align 8
                            char LibFileName[]
bFileName db 'tls2',0
 DATA:00402028
DATA:00402028
                        LibFileName
                                                                                            ; DATA XREF: TlsCallback_Oto
 DATA:0040202D
                                                    align 1000h
 DATA:0040202D DATA
 DATA:0040202D
```



### Am I Missing Somethi

CODE:00401010 push offset LibFileName; "tls2"

CODE:00401005 call j\_LoadLibraryA

CODE:0040100A mov ds:TlsCallbacksEnd, eax

Hmm, LoadLibrary("tls2")
Maybe DllMain contains something interesting?



### I Am Missing Somethi

```
os. IDA - tls2.dll
 File Edit Jump Search
                            View Debug
                                          Options
                                                    Window
 CODE:00400613
                 ======== S U B R O U T I N E ======
               ; BOOL __stdcall DllEntryPoint(HINSTANCE hinstDLL,DWORD fdwReason,LPVOID lpReserved)
                                public DilEntryPoint
               D11EntryPoint
                                proc near
                                        al. 1
                                mov
 CODE:00400615
CODE:00400615 DllEntryPoint
                                retn
                                endp
```

No, that's not it.



#### Take 2

Let's revisit the code:

CODE:00401010 push offset LibFileName; "tls2"

CODE:00401005 call j\_LoadLibraryA

CODE:0040100A mov ds:TlsCallbacksEnd, eax



### It's All About Image

It's the TIsCallBacks extended array trick again.

Q. What value does the new callback contain?

A. The DLL's imagebase.

Q. DEP won't let that run, right?

A. ...



### Surprise!





### Not OK

Of course it will.

You just have to ask nicely.

Or take a cue from a driver.



#### Chaotic-Evil

When the SectionAlignment value is less than 4kb, the file header is marked Writable and Executable (unless the last section characteristics override it).

That turns the ImageBase into code.



#### Before

So we go from this...

```
ox IDA - tls2.dll
                    Search
                             View
                                   Debug
                                           Options
              Jump
                                                     Window
                  ; Segment type: Regular
                                  segment para public '' use32 assume cs:HEADER
                                   jorg 400000h
                                   assume es:_reloc, ss:_reloc, ds:_reloc, fs:_reloc, gs:_reloc
 HEADER:00400000 image_base
                                                             ; MZ_signature ; DATA XREF: HEADER:image_base+3C4o
                                                              HEADER: pe_header+2840 ...
                                   dw OF9E9h
                                                              bytes_in_last
                                   dw 5
                                                               total pages
                                   dw Ø
                                                              num_relocs
                                  dw 4
                                                               header_size
                                   dw OFh
                                                              min_mem
                                   dw ØFFFFh
                                                             : init_SS
                                                              init SP
                                   dw ØB8h
                                   dw 0
                                                             : CRC
                                   dw Ø
                                                              init_IP
                                   dw Ø
                                                              init CS
                                   dw 40h
                                                              relocs offset
                                   dw 1Ah
                                                              overlay number
                                   db 20h dup(0)
                                                              reserved
                                     offset pe_header - offset image_base; new_hdr_offset
```



#### After

To this...

```
ox IDA - tls2.dll
 File Edit Jump Search View Debug
                                                Options Window
                                                                                                                    = IDA View-A
                    ; Segment type: Regular
                                      segment para public '' use32 assume cs:HEADER
                                       ;org 400000h
                                      assume es:_reloc, ss:_reloc, ds:_reloc, fs:_reloc, gs:_reloc
                                                                   ; DATA XREF: HEADER:pe_header+284o; HEADER:pe_header+804o ...
                    image_base:
                                                ebp
                                       dec
                                                edx
                                      pop
                                                loc_400600
                                       imp.
```



#### Presto!

```
ov. IDA - tls2.dll
 File Edit Jump Search View Debug Options
                                                 Window
                              assume cs:CODE
                               org 400600h
                              assume es:_reloc, ss:_reloc, ds:CODE, fs:nothing, gs:nothing
              loc 400600:
                                                      ; DATA XREF: HEADER:pe_section_table to
                               push
                                      offset aDemo
                                                       : "demo"
 CODE: 00400602
                              push
                                      offset aRun
                                                      "eun"
 CODE:00400607
                              push
 CODE: 0040060C
                              push
                              call.
                                       i MessageBoxA
 CODE:00400613
                ----- S U B R O U T I N E -----
 CODE:00400613
 CODE: 00400613
 CODE:00400613
 CODE:00400613 ; BOOL __stdcall start(HINSTANCE hinstDLL,DWORD fdwReason,LPUOID lpReserved)
 CODE: 00400613
                              public start
                                                      ; DATA XREF: HEADER:pe_header to
 CODE:00400613 start
                              proc near
                                                      ; DllEntryPoint
 CODE:00400613
                                      al. 1
                              mov
 CODE:00400615
                              retn
CODE:00400615 start
                              endp
 CODE:00400615
CODE:00400616 ; [00000006 BYTES: COLLAPSED FUNCTION j_MessageBoxA. PRESS KEYPAD "+" TO EXPAND]
                              align 200h
 CODE:0040061C
 CODE:0040061C CODE
                              ends
 CODE:0040061C
```



### Really Not OK

Just a little something to add to the workload.