TLS Callbacks
TLS Callbacks

- What is thread local storage (TLS)?
- We saw this in Chapter 16 on antidebugging.
- What happens if we debug a program that has its malware behavior in a TLS callback?
Debugging Code With TLS Callbacks

- The text noted that one can identify TLS entry points in IDA with ctrl-e (shortcut for menu entry Jump->Jump to Entry Point).
- The text also showed that one could make Olly pause at System Breakpoint (on the Debug->Options Events tab.
- The Olly Advanced Plug-in Makes this easier.
- Selecting the Plugins->Olly->Advanced->Options menu and the checking Break on TLS Callback on the Anti-Debug 2 tab causes the breakpoint exactly at the start of the TLS callback.
In-class Exercise

• Look at sdbot.exe to determine
• What (exactly) is it doing with it's command line argument and where is it doing that?
Next Class

• Carry out Lab 20.3
• Quiz will be based on that lab.