Don’t be helpless: You can put things together, it doesn’t have to be a single command

devblogs.microsoft.com/oldnewthing/20080731-00

July 31, 2008

Raymond Chen

Humans are distinguished among all animal species by their advanced development of and heavy reliance on tools. Don’t betray your ancestors. Use those tools you have.

For example, during the debugging of a thread pool problem, it looked like somebody did a `PostThreadMessage` to a thread pool thread and left the message unprocessed after the thread pool function returned. Who could it have been? Well, one idea was to see if there were any DLLs in the system which called both `QueueUserWorkItem` and `PostThreadMessage`.

I did a little legwork and contributed the following analysis to the mail thread:

> Of all the DLLs loaded into the process, the following call `PostThreadMessage`:
>
> SHLWAPI.dll 77D72436 221 PostThreadMessageA
> SHELL32.dll 77D78596 222 PostThreadMessageW
> ole32.dll 77D78596 222 PostThreadMessageW
> … (list trimmed; you get the idea) …
>
> Of those DLLs, these also call `QueueUserWorkItem`:
>
> shlwapi.dll
> shell32.dll
> … (list trimmed; you get the idea) …

Astounded, somebody wanted to know how I came up with that list.

Nothing magic. You have the tools, you have a brain, so connect the dots.

The `lm` debugger command lists all the DLLs loaded into the process. Copy the output from the debugger window and paste it into a text file. Now write a little script that takes each line of the text file and does a `link /dump /imports` on the corresponding DLL. I happen to prefer perl for this sort of thing, but you can use a boring batch file if you like.

```
for /f %i in (dlls.txt) do ^
@echo %i & link /dump /imports %i | findstr PostThreadMessage
```

Scrape the results off the screen, prune out the misses, and there you have it.

"I tried that, but the result wasn't in the same format as what you posted."

Well, yeah. There's no law that says that I can't manually reformat the data before presenting it in an email message. Since there were only a dozen hits, it's not worth writing a script to do that type of data munging. Typing "backspace, home, up-arrow" twelve times is a lot faster than writing a script to take the output of the above batch file and turn it into the output I used in the email message.

Another boring batch file filters the list to those DLLs that also call `QueueUserWorkItem`. Writing it (or a script in your favorite language) is left as an exercise.

No rocket science here. Just taking a bunch of tools and putting them together to solve a problem. That's what your brain is for, after all.

Raymond Chen

Follow