Finding undocumented swtiches

Posted by Will Steele - 15 Jul 2011 - 21:22

We often work with poorly documented .exe files. How would I find out what undocumented switches exist in a given .exe?

==========

Re: Finding undocumented swtiches

Posted by Robert Kuster - 19 Jul 2011 - 23:12

Hi Will,

what do you mean by undocumented switches? C++ switch-case statements, complier and linker switches, or something else? Do you have sources of these poorly documented applications or just the binaries?

1) In case that you have a binary and that you mean C++ switch-case statements, you could basically disassemble the binary and search for such statements (probably you would write a simple script to automate the process). Usually larger switch-case statements have a so called address-table (see Why should I split up my switch block with more than three case statements?). Your script could then theoretically search for all such places in the disassembled code. Note however that different compilers produce different assembly for the same code and that various compiler switches influence this process extensively too.

A good and widely used disassembler you might consider is IDA.
On top of it Hex-Rays also offers a decompiler. It generates C-code from a binary which would definitely make the search of your switch-case statements much easier.

2) In case that you mean complier/linker switches of binary: Very few of them actually end up in the header of the PE file (for example the image type: exe or dll, the subsystem type: native, windows gui, posix, ..) and could be examined through a PE viewer. However, most of these switches simply determine and influence the way the source code is compiled and linked together into the resulting binary.

I hope this helps,
Robert

==========

Re: Finding undocumented swtiches

Posted by Will Steele - 20 Jul 2011 - 23:55

By switches I mean command passed to the application with the shell. For instance, if I were to use IPConfig, a switch I could use, in this context, is /all to return all IPconfig information. I am thinking this refers to the first case you mentioned above.

==========

Re: Finding undocumented swtiches

Posted by Robert Kuster - 11 Sep 2011 - 16:12

Oh, you mean command line parameters. If you use Process Explorer you could simply click on the process in question and go to the Image tab. For example:
http://windbg.info/images/fbfiles/images/process_explorer_cmd_line_params.png

And in WinDbg you could use the !peb command. It reveals many process related information, among others the command line parameters.

I hope this helps,
Robert

==========

Re: Finding undocumented swtiches

Posted by Will Steele - 12 Sep 2011 - 00:44

Thanks for that tip. I am looking more for what switches are embedded with the image itself. It seems that in C/C++ the command line switches correspond to switch statements within the code. I just have found found what code section I need to check out in the PE or in something like Windbg or Ollydbg to see the switches used to compare against when arguments are passed to the .exe.

==========