How does Microsoft Detours work and how do I use it to get a stack trace?

asked 5 years ago

viewed 11348 times

active 1 year ago

16

I am new to Microsoft Detours. I have installed it to trace the system calls a process makes. I run the following commands which I got from the web

```
syelogd.exe /q C:\Users\xxx\Desktop\log.txt
withdll.exe /d:traceapi.dll C:\Program Files\Google\Google Talk\googletalk.exe
```

17

I get the log file. The problem is I don't fully understand what is happening here. How does detours work? How does it trace the system calls? Also I don't know how to read the output in log.txt. Here is one line in log.txt

```
20101221060413329 2912 50.60: traceapi: 001 GetCurrentThreadId()
```

Finally I want to get the stack trace of the process. How can I get that?

windows detours

share improve this question

edited Dec 31 '10 at 3:42

Rap

4,089 1 26 62

asked Dec 22 '10 at 9:00

Bruce

6,795 35 106 213

add a comment

4 Answers

active oldest votes

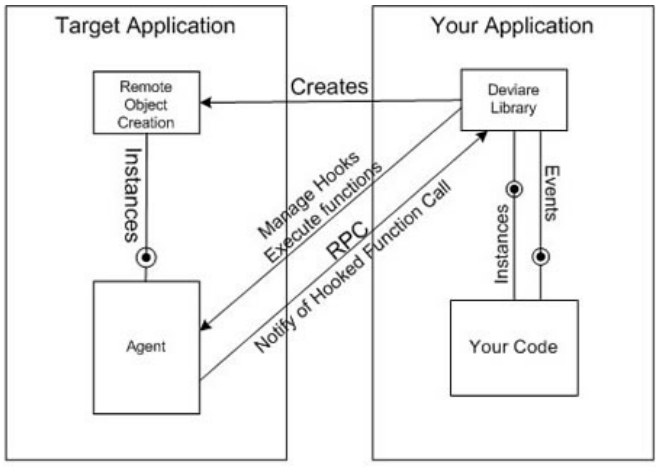
17

Detours lets you intercept any function. It places a jmp in the address that you specify creating a trampoline to your code. Finally, you call the old function if you want to do it. To use Detours you have to inject your code in the process you want to intercept.

To simplify this process you can use Deviare API Hook which does all the injection staff and you can use intercept applications from any programming language that supports COM technology, including .NET, Delphi, C++, Python, etc.. After downloading the package you will find some examples in it. There is a console named DeviareCSharpConsole that let you intercept any API of any process showing full stack trace information.

+50

application that hooks another process:



An agent should be created in the target process to intercept the APIs you want. To intercept these APIs you can use Detours but you have to code IPC staff that is not included in that library.

If you need to write code inside the target process using Deviare API Hook you can use Deviare Custom Hooks. This feature lets you intercept APIs and handle processed parameters asynchronously.

share improve this answer

edited Nov 23 '12 at 14:57

answered Dec 27 '10 at 15:27

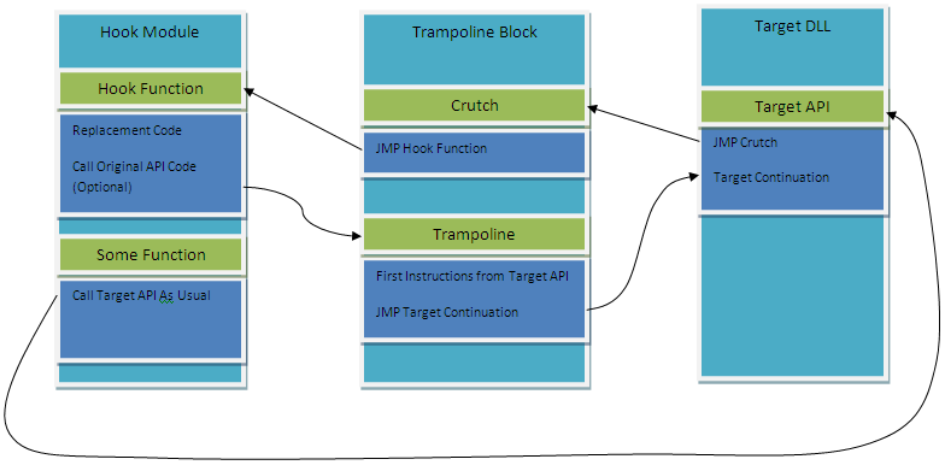
Pablo Yabo
924 7 19

add a comment

17

Instead of detours (which is free for 32-bit only) or easyhook (which is, khm, a *little* bit messy code) you may want to check out mhook 2.4 which is very neat code and BSD-licensed. Works on x86 and x64, handles IP-relative code, etc.

There's also a thorough description on how it works at the site.



As for the stack backtrace, you can use CaptureStackBackTrace() from `kernel32`, or if you want to get fancy, use StackWalk64() from `dbghelp`.

2
Is there a way to make windows output ansi escape sequences

0
Detours: Prevent task kill of my software via another software

2
Why is OSX getting a bus error on an amd64 indirect jump?

Related

5
Microsoft Detours - DetourUpdateThread?

0
Using Microsoft Detours - bunch of undefined's

0
How do function detour packages circumvent security

1
Microsoft Detour - Hook Function with an assembler “call” instruction

1
Having trouble with microsoft detours

0
CopyFile2 not getting detoured

0
detours hooked CreateFile function triggers stack overflow

1
Why does the DirectX Device Present hook not work in detours?

1
How to compile Detours Express 3.0?

2
Microsoft Detours - unable to hook __thiscall function

Hot Network Questions

How do I maximize XP gain?

How much memory is needed to record a human thought?

Could the word "interesting" have negative meaning?

Do AMC have some kind of linkage/negotiation with the British entertainment industry?

How to avoid procedural loops in this example?

Would fewer Jedi be more powerful?

Where am I suppose to actually learn how to compute hypercohomology?

A Canadian with a flat tire

Why is it useful to show the existence and uniqueness of solution for a PDE?

Why must uncommitted transactions be undone in backwards order?

A word for “the shelves of candies or mints next to the checkout desk of a supermarket”

How cheap do prosthetics have to be for poor

edited Nov 5 '14 at 18:40

Johan
45.5k 14 93 188

answered Dec 31 '10 at 6:46

martona
3,542 1 9 15

add a comment

14

First of all, I would HIGHLY advise, that if you want to perform API hooking, I would go with easyhook: http://easyhook.codeplex.com/ (open source). It is a VERY good and easy api-hooking framework.

About how to get the stack trace, I don't remember exactly how to do it, but check out WinAPIOverride32: http://jacquelin.potier.free.fr/winapioverride32/ (open source). He's doing exactly that, and it is open source. Besides, if you need the traces for research, WinAPIOverride32 is a great application to use in order to study how applications work.

EDIT: Just adding one more application. http://www.rohitab.com/ is like WinAPIOVerride32, but it supports 64bit and it really improved since I wrote this answer. I must point out that it in some cases it missed API calls that I found in WinAPIOverride32, but its still pretty good. Unfortunately the source is not published.

About how api-hooking works, Well its a long explanation, I would point you to this article: http://www.codeproject.com/KB/system/hooksys.aspx It gives a pretty good explanation of how it is done under the hood (there are other methods besides what is written there, but still, it is a very good article).

Hope it helps! :-)

share improve this answer

edited Aug 21 '12 at 14:35

answered Dec 25 '10 at 10:48

TCS
2,554 2 25 55

add a comment

2

If you are allowed to use something other than Detours, you could install a debugger like WinDbg and attach it to the process to get a callstack.

You could also try other tools like *Process Monitor* and *Windows Performance Toolkit* as explained here.

share improve this answer

edited Dec 27 '10 at 13:10

answered Dec 26 '10 at 23:05

karlphillip
61.5k 24 142 269

add a comment

Your Answer

SObject
Bash script that lowercases files
Does evolution cost increase?
Why does '() is ()' return True when '[] is []' and '{} is {}' return False?
Tightening Stud Without Bolt Head
Apply Multiple Functions to Parts of a Nested List
Why don't cars have a barrels cylinder head?
Why class size increases when int64_t changes to int32_t
How to perform a proper DDoS test in a safe and controlled way?
Can I just fit a cassette with more gears with the same derailleur?
What is the term for a 3x3 tile set used to create larger areas?
I wrote the code based on a paper's methodology; are there any legal problems with making it open source?

Sign up or log in

Sign up using Google

Sign up using Facebook

Sign up using Email and Password

Post as a guest

Name

Email

By posting your answer, you agree to the privacy policy and terms of service.

Not the answer you're looking for? Browse other questions tagged windows detours or ask your own question.

question feed