Unable to load image ntoskrnl.exe

Posted by Will Steele - 17 Feb 2010 - 18:52

_____

I want to be sure I have WinDbg configured properly. I've got a minidump that returns this error when I load it:

```
Loading Dump File
Mini Kernel Dump File: Only registers and stack trace are available

Symbol search path is: srv*;srv*c:Symbols*http://msdl.microsoft.com/download/symbols
Executable search path is:
Unable to load image WINDOWSsystem32ntoskrnl.exe, Win32 error 0n2
*** WARNING: Unable to verify timestamp for ntoskrnl.exe
*** ERROR: Module load completed but symbols could not be loaded for ntoskrnl.exe
Windows XP Kernel Version 2600 (Service Pack 3) UP Free x86 compatible
Product: WinNt
Machine Name:
Kernel base = 0x804d7000 PsLoadedModuleList = 0x805634c0
Debug session time: Tue Feb 16 10:21:13.427 2010 (GMT-6)
System Uptime: 0 days 1:31:16.250
Unable to load image WINDOWSsystem32ntoskrnl.exe, Win32 error 0n2
*** WARNING: Unable to verify timestamp for ntoskrnl.exe
*** ERROR: Module load completed but symbols could not be loaded for ntoskrnl.exe
Loading Kernel Symbols
.....................................................................
.....................................
Loading User Symbols
Loading unloaded module list
......
ERROR: FindPlugIns 80070015
*******************************************************************************
*                                                                             *
*                        Bugcheck Analysis                                    *
*                                                                             *
*******************************************************************************

Use !analyze -v to get detailed debugging information.

BugCheck 1000008E, {c0000005, 8056ed77, b1813970, 0}

***** Kernel symbols are WRONG. Please fix symbols to do analysis.
```

I have downloaded and pointed to the correct, checked symbols for the OS (XP SP3) and encounter this error. I did glean from another post (http://www.ozzu.com/mswindows-forum/ntoskrnl-exe-errors-t61620.html) that the c0000005 parameter noted in the BugCheck suggests a memory issue. Is there anything I might reconfigure (or download) to get past this error?

==========

Re:Unable to load image ntoskrnl.exe

Posted by Robert Kuster - 18 Feb 2010 - 13:15

Will, Hi.

Unable to load image WINDOWSsystem32ntoskrnl.exe, Win32 error 0n2
For some reason WinDbg doesn't find the associated ntoskrnl.exe image. You usually need both for Crash Dumps:
a) The executable itself (in this case "ntoskrnl.exe"), so that WinDbg is able to show you the disassembly and so on
b) The PDB files -> to get even more information about the executables in question

Here is what I would try to do:
1) put the executable "ntoskrnl.exe" to a place where WinDbg will find it. Take a look at: File (menu) -> Image File Path.

If this doesn't help I would:
2) Change your symbol path: "srv*;srv*c:Symbols*http://msdl.microsoft.com/download/symbols" -> "srv*c:Symbols*http://msdl.microsoft.com/download/symbols"
I don't know if the first srv*; can confuse WinDbg; in any case it won't help either.

3) Enter the following commands to WinDbg:
> !sym noisy
> ld ntoskrnl
> .reload /f /v ntoskrnl.exe

If everything went fine WinDbg will have loaded "ntoskrnl.exe" and its PDB files by now. You can easily check this with one of the following commands:
> !lmi ntoskrnl
> lm vm ntoskrnl

4) If WinDbg still failed to find/retrieve the appropriate files you should at least get a hint of what went wrong because of the "!sym noisy" command (noisy mode - symbol prompts on).
Check 7) Symbols and 10) Loaded modules and image information for more details about the commands mentioned above.

I hope this helps,
Robert

==========

Re:Unable to load image ntoskrnl.exe

Posted by Will Steele - 18 Feb 2010 - 16:37

I feel dumb. While thumbing though the glossary of my copy of Windows Internals I noticed there are two kernel .exe files: ntkrnlmp and ntoskrnl. The first (ntkrnlmp) is for multiprocessor machines. The second (ntoskrnl) is for single processor machines. The light bulb came on and I verified that my machine (a newer dual processor laptop) would not have the single processor .exe. I went to double

check with my co-worker who did in fact say the machine which generated the dump is in fact a single-processor appliance. It was a very simple piece of the puzzle I didn't have. Thanks for the steps I will be sure to keep those close by in case I need them for a real problem. :)

==========

Re: Unable to load image ntkrnlpa.exe

Posted by Chris Cates - 07 May 2010 - 21:04

I have been dealing with a similar issue for several weeks now. We need to run a kernel dump (we are using livekd) on a secure Status server that we CANNOT open up to the internet in order to download symbols from Microsoft's symbols server. We have download the symbols to an identical Stratus server and ran the livekd kernel dump successfully...even moving the symbols directory/path around at will. However, moving the downloaded symbols to another Stratus server (I just keep mentioning Stratus so you guys know I'm talking about identical servers), has a negative result. Even though the command is looking in the correct directory and the symbol is in the directory, the dump still fails. Here's a log file example:

DBGHELP: new session: Fri May 07 12:17:47 2010
DBGHELP: _NT_SYMBOL_PATH: E:WindowsKernelDumpSymbols
DBGHELP: Symbol Search Path: .;E:CtsEftFilesPostilionWindowsKernelDumpSymbols
DBGHELP: .ntkrpamp.pdb - file not found
DBGHELP: .exentkrpamp.pdb - file not found
DBGHELP: .symbolsexentkrpamp.pdb - file not found
DBGHELP:
E:WindowsKernelDumpSymbolsntkrpamp.pdb78B6BD304838400DB0B6EE67B2DB48AF1ntkrpamp.pdb - mismatched pdb
DBGHELP: ntkrpamp.pdb - file not found
DBGHELP: Couldn't load mismatched pdb for ntkrnlpa.exe
DBGHELP: ntkrnlpa - export symbols

We've tried renaming the sub-directory to match the hex string you see above with no success. We believe that Microsoft has configured their symbol downloads to have a unique signature per server (keying off MAC number?). Does anyone know if this is the case or have they had any success downloading symbols on one server and using them on another?

Thanks for any help.

==========

Re: Unable to load image ntkrnlpa.exe

Posted by Robert Kuster - 08 May 2010 - 12:31

Chris, welcome.

We believe that Microsoft has configured their symbol downloads to have a unique signature per server (keying off MAC number?).
Nope. The linker puts a signature (a GUID) into both the executable and the associated PDB as it

creates them. This PDB is valid for this one executable wherever installed.

You mention that one of your computers is on the Internet and the other isn't.
Is it possible that a service pack or KB update installed a new "ntkrnlpa.exe" on one of your computers but not on the other?
Is it really the same "ntkrnlpa.exe" on both machines if you compare them with a hex-editor for example?

We need to run a kernel dump (we are using livekd) on a secure Status server that we CANNOT open up to the internet in order to download symbols from Microsoft's symbols server.
Hm, do you want to create a dump or do you need live kernel-debugging?
For if you just need a DUMP you don't need any symbols. You simply create a DUMP which you then investigate with WinDbg on any other computer which has an Internet connection so WinDbg will obtain the correct symbols from the Microsoft server.
If you on the other side want to do live kernel-debugging: Is it an option to attach WinDbg to your target computer in question, say via Firewire? In this case you only require an Internet connection for your host computer - the one which runs WinDbg (to obtain the symbols). You target computer being debugged doesn't need to be online.

I hope this helps,
Robert

==========

Re: Unable to load image ntkrnlpa.exe
Posted by Chris Cates - 11 May 2010 - 20:08

Thank you for the reply Robert.

I actually found out that the two servers actually had different hardware even though the kernel was the same..stupid oversight on my part. We were able to download the symbols on the 'open' server and test them on a test 'secure' server successfully.

We now need to find out if there will be a descrepancy between Windows Server 2003 R2 sp2 and Windows Server 2003 sp2....

....I'll keep you updated. Thanks again!

-Chris

==========

Re: Unable to load image ntkrnlpa.exe
Posted by Robert Kuster - 28 May 2010 - 15:59

Chris,

you are welcome. I hope you applied correct symbols to all your environments in the meantime.

I didn't try it but I guess you ended up with two different symbol sets for Windows Server 2003 and 2003 R2 respectively... ;)

Warm Regards,
Robert

==========

Re: Unable to load image ntkrnlpa.exe

Posted by Chris Cates - 01 Jun 2010 - 21:49

_____

There does NOT appear to be a descrepancy for the 'R2' variant. We were able to sucessfully download symbols from Microsoft Symbols Server on server A and import/utilize them on server B.

The symbols folder name was 'ntkrpamp.pdb'. There appears to be a dependency on hardware configuration outside of two servers having matching kernels. I found this interesting, but very logical.

Thanks again for your help and letting me bounce this off of here.

Kind Regards,
Chris

==========