

Re: host190.216.26.168.maximumasp.com:80 CLOSE_WAIT

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2005-07/0371.html>

From: Steven L Umbach (*n9rou_at_nospam-comcast.net*)

Date: 07/12/05

Date: Tue, 12 Jul 2005 02:33:26 -0500

If your computer runs fast in safe mode then very possibly you have a startup application/service/driver that is causing the problem. The application/service could be malware/spyware or a legitimate program that is causing a conflict for whatever reason. Troubleshooting such can be a bear because basically you have to do it in a trial and error manner. If you want to try it use msconfig or Autoruns [which probably show more startup processes] to disable startup processes and enable a couple and reboot to see if you can track down the offending process. If it is not a user application it could be a service and you could use msconfig to selectively enable non essential services that are not needed to start up the operating system. If you do that beware that software firewalls are usually installed as a service and if you do not have a hardware device protecting your network you would be vulnerable when the firewall service is stopped. ---
Steve

"lambomadness" <lambomadness@discussions.microsoft.com> wrote in message news:D989FDAA-5F13-413F-89E9-4738979F924D@microsoft.com...

> *Hello Steve,*

>

> *Tried spybot, adaware, CA Etrust, Trendmicro online scan, sysclean like*

> *you*

> *suggested but nothing happened. Only in safe mode is it fast.*

>

> *Have been searching using IE for "explorer.exe high CPU usage" and on one*

> *of*

> *the post it mention of corrupted avi files which cause the system to hike*

> *up*

> *the CPU usage because windows couldn't determine width, height and other*

> *property (which it usually tries to do).*

>

> *I have deleted some avi file from my system, seems to be faster but cpu*

> *usage is still jumping up and down. Currently try to do another scanning*

> *using <http://www.emsisoft.com/en/software/free/>*

>

> *regards,*

> *lambomadness*

>
> *"Steven L Umbach" wrote:*
>
>> *I would use Task Manager or Process Explorer to see if you can find any
>> process that is on your computer that does not exist on a like configured
>> computer that is not having a problem. When you use Process Explorer if
>> you
>> find a process that is mapped to an executable that has no publisher name
>> associated with it that is a red flag though on rare occasion a
>> legitimate
>> process may not show a name. Again if booting into safe mode makes things
>> work a lot better then most likely you have a rouge process on your
>> computer.*
>>
>> *I just repaired my computer where I found a virus running on it. I used
>> two
>> different spyware programs and two virus detection programs and nothing
>> was
>> found. With Process Explorer I found an unknown process running via file
>> named \Windows\mscarrt32.exe that was also using port 1053 as a source
>> port
>> on my computer to attempt to connect to another computer on the internet.
>> The virus was configured to be a service and it also modified my hosts
>> file
>> to show 127.0.0.1 for all the common sites for malware help. I noticed
>> something was up as my computer was sluggish and the command prompt, Task
>> manager, nor registry editor would open. I stopped the service, deleted
>> the
>> associated registry key, and deleted the file. The reason I mention this
>> is
>> that there appears to be more and more malware going around that is not
>> being detected by antivirus programs or at least right away. I suspect my
>> daughter or wife downloaded or opened something and answered "yes" when
>> they
>> should have not.*
>>
>> *Anyhow check for strange processes/services as a start. If you find
>> anything
>> use Google to search for the name of the file you find to see if it
>> brings
>> up anything that may be helpful. Trend Micro has a free tool called
>> Sysclean
>> that may also be worth a try. Just download Sysclean and the current
>> pattern
>> file to a common folder to run from – very easy to do. --- Steve*
>>
>> *<http://www.trendmicro.com/download/dcs.asp> --- Sysclean
>> <http://www.trendmicro.com/download/pattern.asp> -- pattern file in .zip
>> file*
>>
>> *"lambomadness" <lambomadness@discussions.microsoft.com> wrote in message*

>> news:BCF386FE-5893-4717-A73B-B09B67A2F035@microsoft.com...
>> > Thank You Steve,
>> >
>> > I've got tcpview/tdimon from sysinternal and fport from another site to
>> > check out the process and ports. Tcpview shows that SymmTime.exe is
>> > associated with host190.216.26.168.maximumasp.com . Symmtime is a world
>> > clock
>> > and time synchronisation program that I got running on the pcs here.
>> >
>> > I did update the spybot and CA Etrust 7.1.192 and did do a full scan of
>> > both
>> > programs but it didn't found anything. Did disable system restore too.
>> >
>> > Last time I notice something similiar and I decided to reformat the pc,
>> > but
>> > this time, I really do want to know what is bugging it.
>> >
>> > I notice that explorer.exe on my pc is using 25MB of memory and the cpu
>> > column is jumping between 11 and 55 in task manager. This is similiar
>> > to
>> > last
>> > time. I did check with other xp users in our office and they show about
>> > 5MB
>> > of memory usage and cpu is very low (0-2) . Did download the codered
>> > and
>> > mydoom scanner from symantec website but it didn't found anything.
>> >
>> > Even right clicking "My Computer" and the resulting window come up very
>> > slowly, run internet explorer also took sometime to appear. The spybot
>> > scan
>> > is the longest that I could remember to do a full scan.
>> >
>> > regards,
>> > lambomadness
>> >
>> > "Steven L Umbach" wrote:
>> >
>> >> Maximumasp.com appears to be a legitimate website and your netstat
>> >> results
>> >> shows that your computer is connected to their website so that may not
>> >> be
>> >> the problem.
>> >>
>> >> Try using Task Manager or some of the free tools from SysInternals
>> >> such
>> >> as
>> >> Process Explorer, TCPView, and Autoruns to see if you can find any
>> >> rouge
>> >> processes running and with Task Manager look for process or processes
>> >> consuming a lot of memory and/or CPU. It is normal if system idle
>> >> process

>> >> *shows a lot of CPU use however as that actually indicates available
>> >> CPU
>> >> resources.
>> >>
>> >> Try boot into safemode to see if performance increases. If it does you
>> >> may
>> >> have a startup process bogging the system down which could be malware.
>> >> If
>> >> you boot into safe mode with networking be sure that you have a
>> >> firewall
>> >> device protecting your computer as doing such will disable any host
>> >> firewall. I would be sure to do a full scan for viruses being sure to
>> >> update
>> >> your antivirus application to the latest definitions from your vendors
>> >> website and do a full scan with SpyBot using it's latest
>> >> finitions. ---
>> >> Steve
>> >>
>> >> <http://www.sysinternals.com/> --- link to SysInternals.
>> >>
>> >>
>> >> "lambomadness" <lambomadness@discussions.microsoft.com> wrote in
>> >> message
>> >> news:065FF73E-9268-4465-86BA-136232CCA3F9@microsoft.com...
>> >> > Hello all,
>> >> >
>> >> > A couple of days ago, something was trying to edit my host file and
>> >> > spybot
>> >> > s&d ver 1.4 blocked it. My pc is running very slow ever since. As if
>> >> > it
>> >> > is
>> >> > drunk. P4 1.8ghz, 512MB ram , at least 3 gb free hd on both C: and
>> >> > D:
>> >> > (XP
>> >> > sp2
>> >> > with all updates from officeupdate and windowsupdate
>> >> >
>> >> > If pc is connected to the network and sometimes I do a netstat, I
>> >> > can
>> >> > see
>> >> > it
>> >> > establish the connection.
>> >> >
>> >> > Netstat would show:
>> >> > host190.216.26.168.maximumasp.com:80 ESTABLISHED
>> >> >
>> >> > I then pulled out the network cable and do netstat again, then it is
>> >> > gone
>> >> > .
>> >> > tcp mypc:1087 host190.216.26.168.maximumasp.com:80 CLOSE_WAIT
>> >> >*

microsoft.public.security: Re: host190.216.26.168.maximumasp.com:80 CLOSE_WAIT

>> >> > *Anyone seen this problem before or have any suggestion for me.*

>> >> >

>> >> > *Regards,*

>> >> > *lambomadness*

>> >>

>> >>

>> >>

>>

>>

>>

>>