

Win XP RPC Service Failure Reboot Rant Help – the story of a ruined weekend!

Source:

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2004-04/23711.html>

From: dglock (*anonymous_at_discussions.microsoft.com*)

Date: 04/26/04

Date: Mon, 26 Apr 2004 10:38:59 -0700

good luck, bill!
it seems you have already spent as much time as it would
take to start from scratch!
that may be the only way to get out of you problems.
don

>-----Original Message-----

>*Quite a long, complicated story as much to blow off steam
as anything*

>*else, though any help, sympathy or advice would be much
appreciated.*

>*Judging from related threads that I've read here I'm not
the first to*

>*fall foul of this particular problem...*

>

>*If nothing else, this is an anecdote of why it's so
necessary to keep*

>*your OS patched up, a decent anti-virus package
installed, actively*

>*scanning and totally up to date, and your Internet
connection completely*

>*firewalled.*

>

>*Began sometime last week with the decision to upgrade my
existing copy*

>*of Windows ME to XP Home Edition and install Symantec
Internet Security*

>*2004.*

>

>*The catalyst for this decision was my teenage daughter
who saw fit to*

>*install Kazaa because some bright spark at her school had
told her it*

>*was the best way to get free music. As I understand it
now, it's the*

*>best way to get any number of things, most of them being things you
>really wouldn't want to catch...
>
>So, the PC (Win ME, firewalled by Zone Alarm, protected by McAfee VS –
>unfortunately the latter was out of date) could have already been
>infected by the time I took the decision to upgrade. It most likely was.
>However, I suspect I made matters worse...
>
>After uninstalling Kazaa, grounding my daughter for life and booting the
>PC on the Symantec Internet Security CD and letting it take the 34 hours
>it needed to scan for a virus and find nothing, I then ran the Windows
>XP upgrade.
>
>I did this with my Broadband connection active, with Zone Alarm still
>running, because the instructions suggested Windoze would want to
>connect to the Web to download the latest patches as part of its upgrade
>process.
>
>In hindsight, an exceptionally dumb move.
>
>I suspect that the upshot of this is that at some point through the
>upgrade process my Broadband connection became "un-firewalled", as Zone
>Alarm got mangled by XP and XP defaults to not having its own firewall
>active when it first installs.
>
>So ME is now apparently upgraded to XP. I realise that the upgrade has
>mucked up Zone Alarm so uninstall it and switch on the XP firewall.
>Probably too late by now...
>
>Try to install Norton Internet Security. Seems to install fine, but
>doesn't fire up on rebooting. I catch on to this failure eventually,
>uninstall it, switch off the XP firewall (thinking this might be the
>problem) and reinstall it (again, giving myself*

unfirewalled exposure to
>*the Web – Doh!). Of course, no joy.*
>
>*Better still, I start to get the RPC Service sporadically failing and*
>*restarting my computer... Oh, and giving me 60 seconds warning each*
>*time, which I guess could be construed as polite, but personally I think*
>*the bastard PC is just rubbing my nose in it... >:(*
>
>*Some short time later, this leads me (via the web and Microsoft pages)*
>*to the conclusion that I've most likely been affected by W32.Blaster or*
>*one of its variants. This is also the likely reason why Norton Internet*
>*Security is failing to install.*
>
>*I find out how to fix the failure mode of the RPC service so that it*
>*just restarts itself rather than my whole PC, so my PC is now stable*
>*enough to do something with it.*
>
>*I download the Norton W32.Blaster fix and run it.*
>
>*Then I remember I haven't switched the XP firewall back on, and in the*
>*realisation that Norton isn't doing what it said it would do on the box,*
>*I abort the FixBlaster.exe scan and then switch the firewall back on.*
>
>*On aborting the FixBlaster scan it tells me that its found and deleted*
>*one infected file, suggesting that I'm on the right track...*
>
>*Firewall is back on and I restart the FixBlaster scan, now feeling very*
>*optimistic that I'm back on the right track. I have to go out, so leave*
>*my PC to get on with things.*
>
>*The scan eventually finishes, but finds nothing else.*
>
>*Switch the RPC service failure mode back to rebooting the PC on fail,*
>*expecting all to be well once more, and try to reinstall Norton Internet*

>Security... *The RPC service fails, machine gets rebooted.*
Windows again
>*gives me the customary 60 seconds of warning in which to contemplate my*
>*many failures.*
>
>*Oh, and Norton Internet Security failed to install. Same problem as*
>*before. I'm subsequently led by the Symantec site into running MSCONFIG*
>*to try and identify whatever is apparently conflicting with it. MSCONFIG*
>*starts up and gives me a few seconds to speed-read what I can and then*
>*inexplicably closes. A bit like Norton. Well, at least I've identified*
>*the likely conflict.*
>
>*Everything is pointing back at a virus infection.*
>
>*Running the Symantec online scan identifies a couple of hundred files*
>*infected with W32.NetSky – I download the fix from Symantec, run the*
>*scan and let it do its thing. A couple of hundred files are deleted.*
>*Things are looking up?*
>
>*Nope. My old friend the RPC Service continues to reboot my PC with*
>*malicious and mocking glee, MSCONFIG can't keep it up and Norton*
>*Internet Security keeps flopping. Oh, and the Windows Update doesn't,*
>*well, updates. It says it does, it downloads and executes the update, but*
>*on re-running the scan the Microsoft site tells me I still need the*
>*various critical updates I thought I'd just installed. It also leaves*
>*lots of folders in my C:\ with long gibberish names. I imagine those are*
>*the installation files for the various patches and Hotfixes Microsoft*
>*update tried and failed to load.*
>
>*Rerunning the Symantec FixBlaster scan previously downloaded finds*
>*nothing. As of last night, re-running the Symantec Online scan finds*
>*nothing. But the machine is behaving as if it were still*

infected with

>W32.Blaster. I finally went to bed last night in

frustration at about

>3am only to be kept awake by nightmares involving worms,
wooden horses

>and an emasculating inability to bolt the stable door

irrespective of

>the presence of the bloody horse or otherwise.

>

>I haven't downloaded a fresh copy of the FixBlaster.exe
scan from

>Symantec since I first downloaded and ran it on Saturday.

Is it possible

>I've re-infected myself with an updated version of the
virus since then?

>Or the virus has chewed up the FixBlaster.exe? Or I've

infected myself

>with something else entirely that has the same symptoms?

But wouldn't

>the Symantec Online scan have caught something other than
NetSky if that

>had been the case?

>

>Tonight I plan to start again. I've cancelled the various
things I'd

>normally be committed to on a Monday night. Last night's
frustration and

>despair has turned into a quiet anger and simmering
hatred of whatever

>nasty little bug has infected my PC. It's like having
somebody sleep

>with your wife...

>

>So I plan to download a fresh copy of the Blaster fix and
start from

>there, possibly from somebody other than Symantec. And
keep my XP

>firewall active whilst I trawl the web for other ideas,
even though that

>feels a bit like closing the stable door after the horse
has bolted.

>

>If it comes to it, I'll reformat and reinstall everything
from scratch.

>But I really, really hope to avoid that if I can. Some
time back (like

>about two years) I took the decision that backups were
unnecessary, as

>it was only my personal PC, so if I ended up having to
reinstall from

>scratch I wouldn't lose anything critical.

>
>*I was only partly wrong. The data is only one of my*
worries. Having to
>*reconfigure all my applications from scratch, find*
drivers for all my
>*odd bits and pieces like firewire cards and network cards*
and so on, to
>*tweak everything so that it's running just as I like...*
Even the games I
>*play, flight simulators (IL2 rules) and Half-life CTF /*
Day of Defeat
>*for the most part, just reinstalling them and getting*
everything patched
>*just so... Doesn't bear thinking about.*
>
>*Anyway. I apologise for sucking up everybody's bandwidth*
and patience
>*with the sort of tirade to which the obvious response*
is "cry more
>*n00b". But I actually feel a little better now, and ready*
to start again
>*afresh tonight.*
>
>
>*–Bill*
>
>