

Re: Edit Registry from DOS

Source:

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2004-07/21489.html>

From: Incognitus (*in_at_ccurate.com.invalid*)

Date: 07/21/04

Date: Wed, 21 Jul 2004 08:05:21 -0500

"NobodyMan" <none@none.net> wrote in message
news:sshrf05m1ba24445brqr3vv2dcds5ur0mm@4ax.com...

> On Mon, 19 Jul 2004 18:48:06 -0700,

> <anonymous@discussions.microsoft.com> wrote:

>

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

>>Hi All,

>>>

>>>I am attempting to recover from a Spyware install. I've

>>removed the Spyware installation and most registry

>>entries, however, I couldn't remove the most important

>>one until the file was gone. To only way to remove the

>>software was to boot into DOS and delete the file from

>>there since the way it was being loaded was through the

>>WinLogon process.

>>>

>>>The problem I have now is that even though the spyware

>>is gone, I can't remove the entry out of the registry,

>>because my system will no longer boot. In it's current

>>state, when the system boots, it looks for the spyware

>>file during the winlogon process, but since it can't find

>>it anymore, the winlogon process blue screens.

>>>

>>>Before the spyware software was removed, I was unable to

>>delete the entry in the registry, since every time I

>>deleted the registry entry for the spyware, it would re-

>>enter itself. (It had a hook into the explorer.exe

>>process).

>>>

>>>I am now trying to copy the registry from this system to

>>another one so that I can edit it and remove the corrupt

>>entry. I don't know what files the registry consists of,

>>so I was wondering if you could point me to the correct

>>files.

>>>

>>>As an alternative, if any of you are aware of DOS tools

> >I can use to edit the registry, I would also be willing
> >to try that. Note that the entries in the registry for
> >the Spyware are preceded by a null character, so regular
> >registry tools will not even see the entries. I had a
> >heck of a time figuring this out, since essentially the
> >spyware put a null character entry in front of the entire
> >WinLogon registry node. Normal registry tools use the
> >Win32 API, which ignores anything after a null
> >character. In other words, the entire WinLogon registry
> >node in this case.
> >>
> >>At any rate, any suggestions to edit the registry in a
> >>non Windows mode, or by copying it to another computer,
> >>would be highly appreciated. My understanding is that
> >>the spyware was a variation of the VX2 Better Internet
> >>software. Nasty stuff to get rid of, or even find.
> >>
> >>Your help is much appreciated!
> >>
> >>Steve.
> >>.br/>> >>
>
> >XP doesnt have DOS just a DOS prompt. You can also just
> >choose run from the start menu and enter regedit.
> >
> >Better to say XP has a Command Prompt. DOS prompt implies you are
> >accessing MS-DOS via the command line – and as you noted, XP doesn't
> >have MS-DOS.
>

Did you ever wonder why WinXP cmd prompt mem command doesn't know that? :)

>From a mem command using cmd: "MS-DOS resident in High Memory Area".