

Re: Disabling System Restore Points after a successful restore.

Source:

http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.perform_maintain/2006-02/msg00449.htm

- *From:* "Bert Kinney" <bert@xxxxxxxxxx>
 - *Date:* Sat, 18 Feb 2006 14:02:54 -0500
-

Ted Ziegler wrote:

Thanks for the links. My point of disagreement – friendly disagreement, of course – with Jim is on this point that he makes early on:

"...it is better to be able to take a step back to a working version of Windows – even an infected one! – rather than have Windows trashed completely."

For users with limited resources, SR can give them a second chance.

Then again, I'm someone with a comprehensive backup strategy, so wiping out my system and restoring a backup, if it comes to that, is no big deal. These days, I zero confidence in an infected computer.

Like so many other things in computerdom, the answer depends on how well prepared you are. No solution is perfect. (And for the record, in 12 years of personal computing, none of my computers have ever succumbed to infection.)

Obviously, you are an advanced user, and have a strategy in place, just in case. <g>

Restoring back to an infected state is a nice options, when all else fails.

—

Regards,
Bert Kinney MS-MVP Shell/User
<http://bertk.mvps.org>

Re: Disabling System Restore Points after a successful restore.

"Bert Kinney" wrote

Hi Ted and Peter,

This subject has been highly debated. The following comments sum up results and options of the debate, which I agree with.

AumHa Forums: Purging old System Restore points

<http://aumha.net/viewtopic.php?t=15265&sid=f99fc4aceedff192a5242516fe78cd83>

System Restore and malware removal – what is best practice?

<http://msmvps.com/spywaresucks/archive/2005/09/17/66724.aspx>

—

Regards,

Bert Kinney MS–MVP Shell/User

<http://bertk.mvps.org>

Ted Zieglar wrote:

Bert:

Glad you saw this post. I'm a little puzzled by your response, so I hope you can straighten something out for me on this topic.

I have always understood that the possibility that an infected computer's restore points contain a copy of the virus is greater than the possibility that restoring the system would fix whatever problems an antivirus program's removal procedures might cause.

Therefore, if you are fairly certain that you have a virus, you wouldn't want to keep your restore points.

"Bert Kinney" wrote

Rebecca Sansom wrote:

Hi

Sorry I have a bit of a silly question.

I have successfully rolled

Re: Disabling System Restore Points after a successful restore.

back my system using
system restore to
a date before I got a popup
virus that Norton was
unable to
remove. The virus looks like
it has gone from my pc.

I want to now run a
complete virus check and
Norton advises that I
disable system restore
before I do this.

This is bad advise. Disabling System Restore
should be done only
after all infection cleanup is completed. The
reason being, if
something goes wrong (anything is possible)
you will have no way to
reverse your actions. The only way to
re-infect the system is to
undo the current restore point. Update
Norton and do a virus scan.
If Norton finds the virus in the System
Volume Information fold
only, that's the time to purge all existing
restore points by
disabling SR.

This action will delete all
the restore points and I am
therefore
afraid that this will then lose
me the state that I now have
i.e virus free and return the
virus?

No, System Restore does not work that way.
You will only loose the
ability to undo the current state and restore
to a previous date.
The current state of the system will not be
changed by disabling
SR.

Re: Disabling System Restore Points after a successful restore.

Is this the case or can I just go ahead and disable system restore without losing my restored state.

No. By disabling SR it's all or none. Once the system is infection free, other than the System Volume Information folder (where SR holds it's restore points) disable SR, then enable it.

For more on System Restore:
Description of System Restore
<http://bertk.mvps.org/html/description.html>

Any advice much appreciated.

Rebecca

--
Regards,
Bert Kinney MS-MVP Shell/User
<http://bertk.mvps.org>