

# Re: Windows Security Center damaged

---

*Source:*

[http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security\\_admin/2006-10/msg00183.html](http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2006-10/msg00183.html)

---

- *From:* "Gary S. Terhune" <[grystnews@xxxxxxxx](mailto:grystnews@xxxxxxxx)>
  - *Date:* Fri, 6 Oct 2006 16:30:45 -0700
- 

I should have added one more scanner to your list called Multi\_AV (written by MVP David Lipman.) This one runs four different "command-line" scanners, from Sophos, Trend-Micro, McAfee and Kaspersky. It should always be run if you have a confirmed infection (even if whatever you are already using says you're clean.) This page has decent instructions included and the link to download:

[http://www.google.com/url?sa=U&start=1&q=http://harrisonrj.home.comcast.net/step\\_by\\_step\\_pc\\_cleaning\\_process.h](http://www.google.com/url?sa=U&start=1&q=http://harrisonrj.home.comcast.net/step_by_step_pc_cleaning_process.h)

--

Gary S. Terhune  
MS-MVP Shell/User  
<http://grystmill.com/articles/cleanboot.htm>  
<http://grystmill.com/articles/security.htm>

"Gary S. Terhune" <[grystnews@xxxxxxxx](mailto:grystnews@xxxxxxxx)> wrote in message  
[news:ODUMQCZ6GHA.3952@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:ODUMQCZ6GHA.3952@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

"JMZ" <[JMZ@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:JMZ@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)> wrote in message  
[news:E6C08D3A-E1EF-4AB8-A62B-C9DDF9F32D9F@xxxxxxxxxxxxxxxxxxxx](mailto:news:E6C08D3A-E1EF-4AB8-A62B-C9DDF9F32D9F@xxxxxxxxxxxxxxxxxxxx)

Thanks Gary.

I'm not at my home pc right now, so please bear with my generalities as I don't remember the exact wording of everything.

I have Windows XP, SP2. In the Security Center (from Control Panel), there are various options you can select to take different actions. The last option is used to change the way it alerts/notifies you of problems. That option is grayed-out. It does not do anything when clicked. The other options are still functional. So, I'm sure that some malware caused that option to become non-functional, but I think that I have removed that malware

## Re: Windows Security Center damaged

at this point because I don't get the annoying pop-ups from the systray about being infected anymore. The red X is gone. However, the option is still non-functional in the Security Center GUI.

OK, I see what you're talking about. I think you're probably right about the malware being involved. But I'd go through all the steps I advised before, just to make sure. Different malware scanners look for different things, and it takes running several of them to make sure you find it all, finishing off with HijackThis. (There are more in-depth tools, like RootKit Revealer, but you'd use those only on the advise of an expert.) It's possible that one or more of those steps will identify the condition you're seeing as a result of malware and even possibly repair it. I don't know enough about that dialogue to know where to look. Might be Registry, might be some other configuration file or the program itself. I'm not familiar with the programming used here.

My question is how do I make that option functional again? Do you think I need to uninstall and re-install SP2?

I'd not do anything like that until you've done everything else I've suggested and are certain that the malware is truly gone. I'll look into how that dialogue works and how it might be re-enabled. But at this point I consider it a symptom of something that might not have been totally removed. I don't try to fix such symptoms until I'm certain the malware is all gone.

If there is not a setting buried somewhere in the registry, then it may be that application itself was hacked. Would you agree with that? If not, what do you think happened?

Yes, I'd agree that the malware probably disabled the setting in order to disable your ability to be notified. However at this point it's a minor nuisance and not what I'd be focussing on.

BTW, I've already spent \$110 on Norton and NoAdware. If these other programs are similarly priced, then I would sooner buy a new pc.

I'm sorry you did that. The apps I recommend are either free for home use (though donations are always appreciated), or free for a year and \$50(?) after that (ETrust.) EVERYTHING I've recommended you do now can be done

Re: Windows Security Center damaged

with no additional outlay of cash.

Do you think one needs to have all of these tools installed and running, no matter what? It looks like you recommend having 5 to 6 tools, and you didn't even list a firewall, so that's another one.

ETrust Internet Security Suite includes a firewall (built on ZoneAlarm). You can get it for \$30 for the first year, not sure what renewals cost. Maybe \$40 or \$50 per year? Otherwise, use ZoneAlarm (free.) Of course, if you're on broadband you \*really\* want to use a router with NAT firewall included. None of the apps I recommended (except antivirus and now firewall) normally run while you're in Windows. They are either on-demand scanners (you run them regularly to see if anything has gotten in) or they make changes to the system that prevent your IE from going to certain sites, including advertising sites that are embedded in other pages. They add items either to the Restricted Zone or to the HOSTS file. They aren't \*running\* they just add to lists of blocked/restricted sites.

Thanks again.

You're welcome. Keep us posted as to your progress. I'll look up what I can to see if there's a direct repair for that Security Center, but I'm very tempted to not even tell you about it until you've done the things I suggest. I feel that strongly about it.

--

Gary S. Terhune  
MS-MVP Shell/User  
<http://grystmill.com/articles/cleanboot.htm>  
<http://grystmill.com/articles/security.htm>

"Gary S. Terhune" wrote:

"JMZ" <JMZ@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message  
<news:CAD0E5B5-FF63-4224-88A1-436B168C450C@xxxxxxxxxxxxxxxxxxxx>

Thanks for the reply.

No. The popups do not appear anymore and the red X is gone from the

Re: Windows Security Center damaged

systray, but the option in Windows Security Center to change the it notifies me is still grayed-out. Do you think it is still infected or do you think that a malware app I removed already made a change but the removal doesn't necessarily fix that?

I don't understand what it is you're seeing in Security Center. Could you explain that again? Use as much detail as you can to describe to me what you see. In Mine, I see "Security Essentials" and entries for Firewall, Automatic Updates and Virus Protection. I don't see anything resembling whtr I think you're describing.

Do I need more tools than Norton Int Sec 2007 and NoAdware 4.0?

Yes. First, I'd not use Norton at all. Norton is a dumb 800 lb gorilla sitting on top of your system, providing OK protection but interfering with the system on a continuous basis. Causes a lot of problems. McAfee is only slightly better. Use something else like:

ETrust -- <http://my-etrust.com/microsoft>  
Avast! -- [http://avast.com/eng/avast\\_4\\_home.html](http://avast.com/eng/avast_4_home.html)  
AVG -- <http://www.grisoft.com>

Next, I'd use AdAware, Spybot Search & Destroy (scanners that look for malware) and for protection use SpywareBlaster and HOSTS Manager.

AdAware <http://www.lavasoftusa.com/software/adaware/>  
Spybot S&D --

Re: Windows Security Center damaged

<http://www.safer-networking.org/index.php?page=download>  
SpywareBlaster --  
<http://www.javacoolsoftware.com/spywareblaster.html>  
HOSTS Manager --  
<http://www.mvps.org/PracticallyNerded/Software.htm>

If you suspect an infestation is already present, after running all that stuff, then you'll want to run HiJackThis and possibly some others. HJT requires an expert to interpret the results. DO NOT use HJT to "Fix" anything until you're told to do so by an expert. See [www.aumha.org/a/quickfix](http://www.aumha.org/a/quickfix) for more instruction. See, also, the Security link in my sig. (And note that the Clean Boot operations I recommend are for Win98/98SE only. There are similar procedures for WinXP, but I don't get into those. Usually aren't necessary for WinXP, just use Safe Mode instead.

--

Gary S. Terhune  
MS-MVP Shell/User  
<http://grystmill.com/articles/cleanboot.htm>  
<http://grystmill.com/articles/security.htm>

"Gary S. Terhune" wrote:

What you are seeing is almost certainly a malware app. Have you followed through and actually downloaded anything?

See the Security link in my sig, and also <http://aumha.org/a/quickfix.htm>

--

Re: Windows Security Center damaged

Gary S. Terhune  
MS-MVP Shell/User  
<http://grystmill.com/articles/cleanboot.htm>  
<http://grystmill.com/articles/security.htm>

"JMZ"

<JMZ@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

wrote in message

<news:14829952-10E1-4622-896C-F3B87049EFAA@xxxxxxxxxxxxxxxxxxxx>

I use Norton  
Internet  
Security  
2007 and  
NoAdware  
4.0. My  
system is  
(I  
think)  
clean.  
However, I  
did have a  
problem  
with the  
nagging  
security  
center  
pop-ups  
until I had  
everything  
cleaned up.  
The pop-up  
is gone, but  
probably  
only  
because the  
malware tha  
caused it is  
now gone.  
The pop-up  
said my  
computer  
was  
infected and  
I should  
click here to  
install  
software  
to  
clean  
it. When I

Re: Windows Security Center damaged

open  
Security  
Center to  
change the  
way it  
notifies me,  
that  
option is  
disabled.

How do I  
gain full  
control of  
WSC again  
(i.e. get this  
option  
enabled  
again)?

Do I need to  
uninstall  
and reinstall  
SP2?

Thanks in  
advance.