

# RE: Hole in Registry Keys on Office and Windows 2000

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2004-07/0759.html>

---

**From:** InBan (*InBan\_at\_discussions.microsoft.com*)

**Date:** 07/16/04

Date: Fri, 16 Jul 2004 09:18:03 -0700

All of those things are essential in keeping your computer running smoothly and virus/spyware free. The only other suggestion I'd make to home pc users is to use some kind of firewall, especially if you have a high speed connection. Even if its just the ICF built into XP your being protected.

Glad to be a help, surf safe.

Ian

"Dippy" wrote:

> *Hi InBan!*  
>  
> *Thanks for taking the time to explain!*  
>  
> *I keep the Microsoft critical updates and anti-virus stuff*  
> *pretty much up to-date, as also the Spybot and*  
> *Spywareblaster packages that I have installed, but your*  
> *suggestions are good ones.*  
>  
> *Thanks again*  
>  
> *Dippy*  
>  
> >-----Original Message-----  
> >*I'm not from Microsoft.*  
> >  
> >*I've done a little reading up on this. There are plenty*  
> *of discussions on various forums about the DSO Exploits*  
> *Spybot detects. The makers of Spybot have said that this*  
> *is a problem with the current release of spybot and should*  
> *be fixed in future releases.*  
> >  
> >*I have also seen information from other sources saying*  
> *there are registry changes, or an application that can be*  
> *run which makes those changes, which will remove the so*  
> *called DSO exploit.*

> >

> >I would not recommend making those changes. Be confident  
> that the fixes supplied in the critical updates released  
> by Microsoft are fixing these types of issues. Although  
> vulnerabilities in internet explorer likely still exist,  
> far more known vulnerabilities have been patched than not.

> >

> >At this time I would recommend setting spybot to ignore  
> the DSO exploit. I cannot recommend making the registry  
> changes described in other articles and forums as I have  
> not tested them personally, nor am I aware that they do  
> not do more harm than good.

> >

> >If this is related to a real vulnerability in IE it is  
> likely one that is taken advantage of by spy ware makers  
> who would attempt to automatically install software on  
> your computer. The best advice I can give is to avoid this  
> type of hijacking software is – browse safe, I'm sure you  
> know the sorts of sites that these things come from, so  
> just avoid them as a best practice for internet surfing.

> >

> >Good luck.

> >

> >Ian Bagnald

> >MCSE:Security W2K

> >MCSA:Security W2K

> >COMPTIA A+

> >

> >"Dippy" wrote:

> >

> >> Hi InBan,

> >>

> >> Thanx for the advice, below, which I followed without  
> any

> >> success.

> >>

> >> Went to the update page, loaded whatever was marked

> >> critical except for stuff specifically marked for XP or

> >> NT.

> >>

> >> Rebooted, including this evening and again after  
> finding

> >> and installing a Q831167.exe patch that was on my  
> desktop

> >> this morning. (I presume that this was from Microsoft

> >> because it had all the warnings about not installing it  
> on

> >> any machine using pirated software).

> >>

> >> Then Spybot–ted again and there was: the "DSO Exploit"

> >> again and still happily ensconced in my computer.

> >>  
> >> *Are you from Microsoft? If so, what is this "DSO  
> Exploit"  
> >> thing? What does it do, what vulnerabilities does it  
> open–  
> >> up and why can't you get rid of it?*  
> >>  
> >> *Thanxs again and looking forward to growing wiser, as I  
> >> will be once you – or Microsoft – find a way to crack  
> this  
> >> one!*  
> >>  
> >> *Dippy*  
> >>  
> >>  
> >>  
> >>  
> >> >-----Original Message-----  
> >> >*Make sure you have all of the latest critical updates  
> and  
> >> service packs.*  
> >> >  
> >> >*Ian Bagnald*  
> >> >*MCSE:Security W2K*  
> >> >*MCSA:Security W2K*  
> >> >*COMPTIA A+*  
> >> >  
> >> >*"Dippy" wrote:*  
> >> >  
> >> >> *I run office and Windows 2000 on a 500 Pentium III  
> PC  
> >> with  
> >> >> 256 megs of ram and a 75 gig harddrive. Intel chip  
> and  
> >> >> motherboard.*  
> >> >>  
> >> >> *I was warned about the proliferation of spyware and  
> >> >> downloaded Spybot 1.3 Search and Destroy freeware  
> from  
> >> >> Tucows.*  
> >> >>  
> >> >> *It seems to have weeded–out all manner of assorted  
> junk  
> >> >> except for one that remains hanging in the air, just  
> >> like  
> >> >> a bad smell.*  
> >> >>  
> >> >> *At the end of every scan, after 'Immunization', it  
> >> always  
> >> >> shows, every single solitary time, that it has*

> *picked-*  
> > > *up*  
> > > > *an item that it lists as:*  
> > > >  
> > > > *DSO Exploit*  
> > > >  
> > > > *Under details, it shows the following message:*  
> > > >  
> > > > *DSO Exploit: Data source object exploit (Registry*  
> > > *change,*  
> > > > *fixed)*  
> > > > *HKEY\_USERS\S-1-5-21-1343024091-1383384898-*  
> *1708537768-*  
> > > *500*  
> > > > *\Software\Microsoft\Windows\CurrentVersion\Internet*  
> > > > *Settings\Zones\0\1004!=W=3*  
> > > >  
> > > >  
> > > > *--- Spybot - Search && Destroy version: 1.3 ---*  
> > > > *2004-07-09 Includes\Cookies.sbi*  
> > > > *2004-07-09 Includes\Dialer.sbi*  
> > > > *2004-07-09 Includes\Hijackers.sbi*  
> > > > *2004-07-09 Includes\Keyloggers.sbi*  
> > > > *2004-05-12 Includes\LSP.sbi*  
> > > > *2004-07-09 Includes\Malware.sbi*  
> > > > *2004-07-09 Includes\Revision.sbi*  
> > > > *2004-07-02 Includes\Security.sbi*  
> > > > *2004-07-09 Includes\Spybots.sbi*  
> > > > *2004-07-09 Includes\Tracks.uti*  
> > > > *2004-07-09 Includes\Trojans.sbi*  
> > > >  
> > > > *This leads to some information to the effect that*  
> *there*  
> > > *is*  
> > > > *a 'hole' that has not been closed by Microsoft,*  
> > > *referring*  
> > > > *again to a Microsoft home link, a Microsoft Security*  
> > > *link*  
> > > > *and a Microsoft '.windows/-ie' link.*  
> > > >  
> > > > *Needless to say, I find it impossible to actually*  
> > > *contact*  
> > > > *those folk!!!!? (I'm sure I'm not*  
> *alone.....!!!)*  
> > > >  
> > > > *There is also a note about a link*  
> > > > *to '<http://security.greymagic.com/adv/gm001-ie/>' for*  
> > > *more*  
> > > > *information. This expands to say that there is*  
> *a 'hole'*  
> > > *or*

> >> >> *flaw in the system, but I know zip about computers –*  
> >> *and*  
> >> >> *even less when there is any kind of glitch – it is*  
> >> >> *meaningless to me.*  
> >> >>  
> >> >> *Can anyone throw any light on this for me in*  
> *layman's*  
> >> >> *terms, as it seems that Microsoft either can't or*  
> *won't*  
> >> >> *fix it, from the looks of things.*  
> >> >>  
> >> >> *Thanks all!*  
> >> >>  
> >> >.  
> >> >  
> >>  
> >.  
> >  
>