

Re: Cleaned a badly infected PC, upgraded to SP2, and OE inbox overwritten!

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.inetexplorer.ie6_outlookexpress/2004-10/1

From: Bruce Hagen (*Nospam_at_mymail.invalid*)

Date: 10/07/04

Date: Thu, 7 Oct 2004 08:59:54 -0700

This KB article is for lost e-mail after upgrading to XP, but many have had success following the same procedure when messages were lost after downloading SP2:

<http://support.microsoft.com/default.aspx?scid=kb:en-us:313055&Product=winxp>

Bruce Hagen
MS MVP – (IE/OE)
~IB-CA~

"Mitch" <anonymous@discussions.microsoft.com> wrote in message news:172601c4ac6c\$a53a66d0\$a401280a@phx.gbl...

- > *Hey all. Wondering if you can help. I was working on a*
- > *client's computer; massive multiple worm infections*
- > *(Beagle, Blaster, MMail, MyDoom). I see a lot of these*
- > *sort of infections in my business, and have repaired many*
- > *such boxes.*
- >
- > *What was different this time is that after all the worms*
- > *were removed, the registry cleaned, antivirus software*
- > *installed, etc., I went ahead and upgraded the (XP) box*
- > *to SP2 to patch the various holes that led to the*
- > *infestation in the first place.*
- >
- > *Everything went smoothly, but after reboot, I fired up*
- > *Outlook Express (inability to download mail was what led*
- > *to the call in the first place), and everything in the*
- > *inbox was suddenly gone. Five new messages downloaded.*
- >
- > *So I starting cussing and frantically searching the*
- > *entire computer for any instance of .dbx files. There was*
- > *only one inbox.dbx, however, and it was now but 1 meg in*
- > *size (whereas it had been over 100 meg before). I tried*
- > *running DBXtract on all the dbx files, but the only*
- > *messages extracted from the inbox were the five new*

- > *messages.*
- >
- > *I'm assuming the inbox had been overwritten, and I*
- > *wouldn't be surprised if it were a defense mechanism*
- > *built in to one of the worm variations on the box, but my*
- > *question is this: is there any way y'all know of to*
- > *retrieve overwritten dbx files?*
- >
- > *thanks for any help.*
- > *mc*