

Re: WindowsUpdate V5 on XPSP1 broken

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2004-09/0102.html>

From: David Sentelle (*David.Sentelle_at_CNBCBANK.COM*)

Date: 09/29/04

Date: Wed, 29 Sep 2004 13:13:39 -0400
To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

Thanks for forwarding these.

You might want to also inform people that some viruses/trojans/adware/spyware will block windows update. When the original email on this thread came in, I was in the process of scanning a drive for nastiness, of which ~80 different things were found, all classified by Norton 2005 or Symantec AV CE v9 as being ad/spyware.

No official viruses. :)

My cleaning attempts.... after cleaning from the booted drive....

Plug it in as a secondary drive in a good system, thoroughly scanned & cleaned with Symantec AV CE9.0 & Ad-Aware Pro (both with current sig files)

Some files were found which could not be deleted in this situation. I had to go change ownership of the files, then the attribs could be changed and the files deleted.

Scanned it again. Appeared clean in both SAV & AdAware

Then booted and ran Norton 2005 & Ad-Aware, 2 items found.

Manual removal was possible. Rescanning looks clean.

Ran the toolbarcop

(<http://www.mvps.org/sramesh2k/toolbarcop.htm>) and removed everything.

Rescan everything looks clean. Homepage still hijacked and windowsupdate fails, still stating that activex isn't allowed.

Needless to say, I've added all the appropriate sites to the 'trusted sites', as well as tried with internet security settings set at low.

At this point the MSIE homepage still gets hijacked, and Windows Update gets blocked.

Amazing.... no viruses... Just adware. It should be a crime.

I'm telling the guy to go home and burn copies of everything he needs, without plugging into the net, and bring it back with the restore CDs.

All this because he let a nephew on his PC during a visit. This nephew

NT-Bugtraq: Re: WindowsUpdate V5 on XPSP1 broken

apparently likes casino sites. <g>

--

NTBugtraq Editor's Note:

Want to reply to the person who sent this message? This list is configured such that just hitting

--