

NT-Bugtraq: MyDoom/Zindos removal tool offered erroneously via AutomaticUpdates?

MyDoom/Zindos removal tool offered erroneously via AutomaticUpdates?

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2004-08/0046.html>

From: Glenn Turner (glenn_at_GLENN-TURNER.COM)

Date: 08/13/04

Date: Fri, 13 Aug 2004 09:11:37 +1000
To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

On one of my home PCs – which is behind the correctly-configured firewall in my dsl modem, and also uses the Windows XP firewall, – and which always gets updated with AutomaticUpdates, has (and always has had) up-to-date virus protection, I was offered the MyDoom and Zindos Removal tool in WindowsUpdate as a Critical Update.

<http://support.microsoft.com/?kbid=836528>

I clicked on the more information link and was told that if I'm being offered this, it is because I'm likely infected with the worm.

Anyway, (surprise surprise), running the tool didn't find any infection. Neither did a full scan with Norton Antivirus using current definitions.

Has anyone else been offered this download? I'd love to know what criteria they used to determine I was infected.

I note that Zindos.A is used to create a date-triggered DoS attack against Microsoft.com.. perhaps they are being over-cautious..

Glenn

NTBugtraq Editor's Note:

Want to reply to the person who sent this message? This list is configured such that just hitting reply is going to result in the message coming to the list, not to the individual who sent the message. This was done to help reduce the number of Out of Office messages posters received. So if you want to send a reply just to the poster, you'll have to copy their email address out of the message and place it in your TO: field.
