

Re: Infected files in VSS

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2004-07/5365.html>

From: Gavin (gavin_at_inteNOorproSPAMm.com)

Date: 07/21/04

Date: Wed, 21 Jul 2004 19:46:55 -0400

Hi Trev,

The virus got it BECAUSE it's excluded ;)

What happened is that the virus wasn't scanned or captured via the hard drive because it was excluded, HOWEVER, the VSS version of the file WAS scanned because Trend is seeing it as a proper file, but not one that's part of your exclusion list.

This seems to be popping up more lately. Diligent planning and configuration of quarantined directories, mail queue's, etc are essential.

--

Gavin [SBS Consultant]

<< SBS ROCKS !!! >>

"Trevor OE News" <thetrev68 @ hotmail.com> wrote in message news:ua8mNn1bEHA.2844@TK2MSFTNGP12.phx.gbl...

> Gavin,

>

> I don't see your post below, but I had the same thing happen in the last 2
> days. I solved it by disabling shadow copies and re-enabling it. The
> shadow copy tab is in the properties of your hard drive when you
> right-click it in windows explorer.

>

> In my case, Trend announced WORM_NETSKY.P was in the following folder:

>

> Infected file: \Device\HarddiskVolumeShadowCopy69\Program
> Files\Exchsrvr\Mailroot\vsi 1\Queue\NTFS_1af3611001c46dbd00004549.EML

>

> The notice repeated every time VSS ran. Same for you? It also killed my
> nightly backup with an "access denied" message.

>

> Note: I do have the mailroot folder excluded from OfficeScan. I'm not
> sure yet how the virus got in.

>

> -Trevor

>

> "Gavin" <gavin@inteNOorproSPAMm.com> wrote in message
> news:exSuPW1bEHA.904@TK2MSFTNGP09.phx.gbl...

>> If an infected file ends up in System Restore under Windows XP, the
>> proper way to get rid of it is to turn OFF system restore, which deleted
>> the "cached" files, and then turn it on again.

>>

Re: Infected files in VSS

microsoft.public.windows.server.sbs: Re: INfected files in VSS

```
>> What is the similar procedure in SBS 2003 where an infected file -  
>> although deleted from the drive - is still "hanging out" in the volume  
>> shadow copy stored data - or will it disappear at the next refresh?  
>>  
>> (Note; See my post below regarding this happenstance)  
>> --  
>> Gavin [SBS Consultant]  
>>  
>> << SBS ROCKS !!! >>  
>>  
>>  
>  
>
```