

## Re: virus in blob file

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.sqlserver.security/2004-12/0115.html>

---

**From:** John Bell ([jbellnewsposts\\_at\\_hotmail.com](mailto:jbellnewsposts_at_hotmail.com))

**Date:** 12/13/04

Date: Mon, 13 Dec 2004 18:14:51 -0000

Hi Riccardo

See comments inline:

"Riccardo" <[Riccardo@discussions.microsoft.com](mailto:Riccardo@discussions.microsoft.com)> wrote in message news:2635B145-DBB1-4A3E-876A-8B51A4AC3C51@microsoft.com...

> *Dear John,*

>

> *I'd like to evitate to write in the file system a potetially dangerous file.*

If your server is protected correctly then you should be running the latest virus detection software as a matter of course especially if you are connecting to the internet, therefore it should not be a problem, especially if you sandbox the area this is going to write to.

>

> *1. if i don't use a method to prevent the virus attach by means of uploaded*

> *files, the server is sure, because the virus is stored in the DB, and so*

> *it's*

> *not able to attack the system.*

I would not be sure of that, any assumption is a potential vulnerability that someone will exploit.

> *On the other side, the client that downlaods*

> *an uploaded infected file can be infected. So this solution is sure for the*

> *server, but not for the client.*

You can not guarantee that any client is safe unless this is a totally closed system.

>

> *2. If I uses your solution, I've to write a potentially dangerous file in the File System. Two problem:*

> *2a. performance*

Performance of the database when writing large blobs into it may also be an issue. Writing to the file system will mainly be dependent on the hardware, you are not necessarily going to write the files to your database server, and therefore you would have to analyse volumes and usage and do some

benchmarking before writing this option off..

> *2b. If the virus is newer than the virus definition in the antivirus, I*

> *can*

> *write in the file system a dangerous file....*

> *This solution is good for the client, but not enough for the server.*

I am sure some AV software has some interface/component you can tap into, but you will always be reliant on the services of your AV provider regardless of where the file is stored.

>

> *What do you think about?*

>

> *Thanks,*

> *Riccardo.*

HTH

John

>

> *"John Bell" wrote:*

>

>> *Hi*

>>

>> *If they are uploaded then they must be materialised on the webserver or*

>> *database server, therefore they can be scanned before importing.*

>>

>> *John*

>>

>> *"Riccardo" <Riccardo@discussions.microsoft.com> wrote in message*

>> *news:6AC90389-C8CB-4834-B0E0-4AD8BFF57DBD@microsoft.com...*

>>> *Hi!*

>>>

>>> *I'm developing a three tiered application based on .NET and SQLServer. I*

>>> *use*

>>> *SQL Server 2000 to store files uploaded by user by means of a web based*

>>> *ASP.NET application.*

>>> *How can I prevent the upload of infected files in the DB? Does it exist*

>>> *an*

>>> *antivirus that can scan the files stored in the BLOB files of the DB?*

>>> *Install a virus wall in a proxy is the only one solution for preventing*

>>> *virus upload and download?*

>>>

>>> *Thanks,*

>>> *Riccardo*

>>

>>

>>