



Don't Rely on an Anti-virus Program To Keep Your IFS Safe

Most people with knowledge of the iSeries know that while a virus cannot run in the OS/400 operating system or file structure, a virus or worm can still get into your iSeries, specifically, into the IFS integrated file system. A virus which has found its way to one of your connected PCs doesn't even need to be duplicated in the IFS to cause damage. Once there, it can execute in Windows, Linux or Unix, without the PC's user being aware of it. The road is then clear for it to delete or corrupt the files in the IFS.

The anti-virus technologies can go some way towards protecting against this. They can scan the computers drives, including the mapped iSeries drive, in an attempt to identify known virus signatures and additionally identify virus-infected programs at execution time. However, as fast as their producers may be at picking up (and cashing in on) the latest virus to hit the web, their powers of protection are severely reduced or non-existent (depending on their heuristic capabilities) for unlisted viruses. Not to forget either, that the PC's owner must regularly update the virus list, schedule regular scans and make sure the anti-virus software is always up and running.

Reports recently published indicate the Mydoom.f virus was responsible for the deletion of some 25,000 files from one iSeries installation's IFS directories. In other cases, a similar virus was found in email messages stored on the iSeries. There are a couple of interesting points stemming from the deletion incident that might just have got missed. Firstly, the virus was unquestionably executed by a connected PC and secondly, the anti-virus program ON THE PC either did not run or ran without succeeding in catching the virus. The virus may not even have been replicated on the IFS. As explained above, the corruption / deletion of these files was more due to the easy reach of the IFS by the PC, rather than whether the virus got copied onto the IFS or not.

But it isn't just well-known viruses that can create havoc on your computer. Lesser-known viruses or other malicious software might be just as damaging, if not more so. Windows (DOS) batch files for example, can be easily created containing commands to rename, delete and move files by generic name. Hundreds, even thousands, of files can then be compromised in a single command. An angry worker, part-time hacker or careless programmer might just run such a program on a PC having access to the IFS. Commands like `erase g:*.*`, `rename h:branch*.dat *.tmp`, and `move f:d*.* g:` can spell big trouble. They can lose thousands of files in a single command and this kind of program is not so easily caught.

© Copyright 2004 Bsafe Information Systems, Ltd. All rights reserved. This document is the property of Bsafe Information Systems, Ltd. It cannot be passed on to any party, individual or organization without the express permission of Bsafe Information Systems. www.bsafesolutions.com

Tel: 905-763-8214 (Canada) 800-346-1055 (US / Canada only) +972-9-9525480 (All regions)



It is somewhat fortunate, therefore, that OS/400 does give us some flexibility to monitor the gateway through which IFS files are accessed. That gateway is called the iSeries file server and can be controlled through the file-server exit-point.

Bsafe/Global Security for iSeries utilizes this strategic security 'check-point' to implement a whole structure of controls which would prevent the above batch file commands from causing the damage they were intended (or unintended) to do. For starters, you can restrict all operations of all kinds for all users by simply not allowing any request to pass. That way you close the IFS and its integrity is protected. Of course, that rather defeats our aim of making use of the IFS. So, after restricting everyone, you would allow appropriate kinds of action to selected users like read, delete, create etc., much like you would for OS/400 objects.

Once you have locked out all users except those who really need to use the IFS you're still faced with two major problems. The first is you haven't yet restricted specific IFS paths to specific users. This is equivalent to restricting appropriate libraries to appropriate users in OS/400. The second is probably the most critical weakness of all and possibly the one that allowed the 25,000 files to get deleted by a virus. Those very same PCs, whose users who have been given the rights to create and delete files in the IFS, may run the virus or malicious program, or commands. All it takes is a moment the PCs unsuspecting user is away from the desk for a perpetrator to run the malicious code, or insert it so the unsuspecting user will run it later. When the PC is accessible by others from the network, the intruder doesn't even have to wait for the opportunity of an unmanned PC.

These problems are easily handled by Bsafe/Global Security. Specific paths and specific functions may be allocated to specific users. A detailed log is available to register all activity so excessive deletions could trigger an alert to indicate a malicious program or virus.

This kind of solution provides a level of protection where the anti-virus scan cannot, whether it is executed on the iSeries server or the PC client.

In addition, Bsafe/Global Security is enhanced with additions to make an all-round security package making it a powerful and flexible addition to your security implementation.

Details of the product are available at the Bsafe Solutions website www.bsafesolutions.com.

For more information contact us on chaya@bsafesolutions.com or phone one of the numbers below.

© Copyright 2004 Bsafe Information Systems, Ltd. All rights reserved. This document is the property of Bsafe Information Systems, Ltd. It cannot be passed on to any party, individual or organization without the express permission of Bsafe Information Systems. www.bsafesolutions.com

Tel: 905-763-8214 (Canada) 800-346-1055 (US / Canada only) +972-9-9525480 (All regions)