

Re: How to block system copy commands at driver level

Source:

<http://www.tech-archive.net/Archive/Development/microsoft.public.development.device.drivers/2008-05/msg00748.1>

- *From:* "Don Burn" <burn@xxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 23 May 2008 08:01:22 -0400
-

And the answer is there are no basic copy commands. All you are going to see are reads and writes, there is no concept of copying at the kernel level. So unless you want to make a file so it cannot be read (which makes it rather useless) you cannot stop copying. Go to <http://www.osronline.com/> and join the NTFSD newsgroup, and then start reading the archives, this has been discussed way too many times.

--
Don Burn (MVP, Windows DDK)
Windows 2k/XP/2k3 Filesystem and Driver Consulting
Website: <http://www.windrvr.com>
Blog: <http://msmvps.com/blogs/WinDrvR>
Remove StopSpam to reply

"Bipin Mistry" <bpnmistry@xxxxxxxxxx> wrote in message
news:7b8f425d-e3c1-41c5-a321-5cb18c07899b@xx
Hello David,

Up to the extent I agree with you that this task can not be done unless we know how Windows works with these events at low level.

Put the data to be protected in a directory. Encrypt that directory's files with a symmetric key or multiple keys. Store those keys on a SmartCard protected with the public key used to encrypt them before they are added. Issue a CD/DVD/USB drive with the files on it, a SmartCard reader, & the fully initialized SmartCard. Write an application that permits the files to be viewed, but does not respond to any key strokes that might copy the data in the viewer.

Re: How to block system copy commands at driver level

Hello,

How can I trace following System Copy commands and block them, so as secured folder/drive do not react to these commands.

1. [Ctrl + C],
2. Right Click Menu -> Copy
3. File Menu -> Copy
4. Command prompt copy

As per me all above command will be calling a single routine process at driver level.

I am unable to identify which routine dose it call & how can I identify that the any of above 4 are triggered.

During my RnD till now I reached till IRP_MJ_READ & WRITE where by related parameters and their properties do not describe about COPY in specifically.

Some place I read about this can be posible with keeping watch on Clipboard, dont know how much this will be useful, as there was no extra informaiton was provided.

If any one can help me out for this situation then please do share your knowledge with me.

Best regards,
Bipin- Hide quoted text -

- Show quoted text -