

RE: Restrict Access to drives

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2002-02/0141.html>

From: Jorge Roxo (j.roxo@sotagus.pt)

Date: 02/20/02

From: "Jorge Roxo" <j.roxo@sotagus.pt>

To: "'Shane Singh'" <netadmin@mazenod.vic.edu.au>, <focus-ms@securityfocus.com>

Date: Wed, 20 Feb 2002 08:22:21 -0000

Hi Shane,

The reason for this is very simple, Windows 2000 and Windows XP, actually any NT tech based machine performs a so called "administrative share" of HDD drives. By restricting access to the hdd to your users basically what you have done is to prevent them from accessing their "share" of the documents and settings folder. Thus their logon fails, since they cannot access the information on the hdd that would make the logon complete.

The solution to this is simple, you may re-share the drive but stating which user has access to what folder. In simpler terms, you may grant access as per local security policy to the default documents and settings folder as well as to the temp dir on the windows directory and some other folders which may be necessary.

We have implemented a similar policy, allowing only certain users to view and alter the hdd contents (namely local administrator users) through the use of the security groups provided in Windows 2K Pro and XP pro.

By effectively implementing the user group policy settings you achieve the same results, but they may in the long run prove to be more of a hassle than a benefit since, for instance, if you where to try to run an update program for say, Panda Antivirus in a Win 2K Pro or Win XP pro machine the user that's logged on would need to be at least an advanced user type or else the program that by updating must modify a certain number of critical files will not be allowed to do since it has not got enough privileges.

Basically you should stick to preventing access to determinate user to certain folders, not to the whole hdd. Try preventing general user access to Windows/System32 and you'll get an idea of what I mean.

Another good idea is to set a user with advanced or local administrator privileges as the owner of certain folders which you may consider to be

SecurityFocus Microsoft: RE: Restrict Access to drives

sensitive enough that you do not want people messing in them, thus allow access to System and administrator for instance, and you'll see most stuff will run fine where as the users will have access denied to those folders.

Hope it helps some....

Jorge Roxo,
TCSA/Sotagus Computer Systems Administrator

This e-mail is confidential and privileged. If you are not the intended recipient please accept our apologies. Do not disclose, copy or distribute information in this e-mail or take any action in reliance to its contents, to do so is strictly prohibited and may be unlawful. Please inform us that this message has gone astray before deleting it. Thank you for your co-operation.

-----Mensagem original-----

De: Shane Singh
Enviada: quarta-feira, 20 de Fevereiro de 2002 0:41
Para: focus-ms@securityfocus.com
Assunto: Restrict Access to drives

I'm hoping someone can shed some light on this annoyance.

I have restricted access to local hard drives for users but when they log in they get a message stating "Operation Cancelled due to restrictions on this Computer". This also happen in some software when they try using a dropdown box for opening/saving data.

Is there a way to remove this message via registry, etc. while still keeping the restrictions in place?

Thanks,
Shane Singh
Systems Engineer
Microblue Pty Ltd
sysadmin@mazenod.vic.edu.au
www.microblue.com.au

-
- **Previous message:** [Olav Seyfarth: "Re: Cached Domain Password on Notebook, secure?"](#)
 - **In reply to:** [Shane Singh: "Restrict Access to drives"](#)
 - **Next in thread:** [Bill Mote: "RE: Restrict Access to drives"](#)
 - **Reply:** [Bill Mote: "RE: Restrict Access to drives"](#)
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)