

Re: Disabling Execute access in Documents and Settings?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2004-06/0748.html>

From: Steven L Umbach (*n9rou_at_nospam-comcast.net*)

Date: 06/20/04

Date: Sun, 20 Jun 2004 02:59:09 GMT

I like the idea about disabling execute for files only in a user profile and may be helpful in locking down a computer to unauthorized application use as many users do that in their profile if their computer is configured to only allow them to write to their profile by modifying ntfs permissions for everyone/users for the root/drive folder.

Windows XP Pro of course uses Software Restriction Policies to control what can and can not be executed on a computer by a user. I don't know of any way to change the default profile permissions assigned to a user when their profile is created, though a startup script using fileacl may be able to configure to your needs as it seems to have the ability to configure special permissions and it is an official MS support tool now. I really like the fact that it has an inherit and protect switch that makes some advanced folder configuration possible. --- Steve

<http://membres.lycos.fr/jfb/gb/gbtools/fileacl.htm>

<http://www.microsoft.com/downloads/details.aspx?FamilyID=723f64ea-34f0-4e6d-9a72-004d35de4e64&displaylan>

"Gordon Fecyk" <gordonf@pan-am.ca> wrote in message

news:O4x096jVEHA.1656@TK2MSFTNGP09.phx.gbl...

- > *Someone showed me a neat trick that takes advantage of a recent IE6*
- > *cross-site scripting vulnerability. The trick successfully copied an*
- > *executable to %userprofile%\Start Menu\Programs\Startup.*
- >
- > *Neat little trick, though the executable's still bound by the permissions of*
- > *the user logged on. But the area is writable and executable to the user in*
- > *question.*
- >
- > *The obvious before-the-fact fixes include:*
- >
- > ** System or Group Policy defining which executables may be run*
- > ** Disable scripting for the My Computer zone and stick to the "Classic"*
- > *Explorer Shell (Registry setting, either Policy or Default Profile)*
- > ** Disable personal program groups / Start Menu items (but does nothing if*