

Server has been hacked, need to delete hidden user account

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2007-05/msg00116.html>

- *From:* "Øyvind Isaksen" <hojoi@xxxxxxxxxx>
 - *Date:* Fri, 25 May 2007 11:44:00 +0200
-

I need urgent help! My windows 2003 server has been hacked. When I was defragmentating my disks some files could not be defragmentated. I discovered that the reason is because these files is created on a userprofile called "superwayne\$" at this location C:\Documents and Settings\superwayne\$. If I open this address in Explorer, I see folders like "desktop", "Favorites", "Local Settings", "superwaynes's Documents" and so on. There is alot of hacked software, movies and other stuff in these folders.

If I open Active Directory Users and Computers, the user "superwaynes\$" is not there. In Server Management/Users I cant find this either. It seems like the user "superwaynes\$" has been created outside my domain or something. How can I find and delete this user profile (not only the files in C:\Documents and Settings\superwayne\$)? How could this happen, what can I do prevent this in future? My server has only licensed software (no hacks), only I got access to it?