

Re: lsass.exe in CPU loop when logging in

Please note that before you do this you should run: CHIPHER /H /N /U
This will identify all encrypted files on your local drive. You need to
decrypt them before you
remove the contents of the Protect directory (on an XP system the files
are in a directory with a
GUID for a name under the Protect directory). Once you remove the
contents of the directory you
cannot decrypt files that were encrypted earlier. You can still encrypt
files after you empty the
directory and you will be able to decrypt those.

Stu

"Joe Hubele" <Joe.Hubele@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote:

Thanks to this posting, I realized I had also copied encrypted
files
causing
lsass.exe to take over the system for several minutes after
logon. The
problem profile was a member of the administrators group
and so I did
not
suspect a security issue.

I decrypted the local files and disabled EFS but it did not
help. After
a
lot of searching and head scratching, I finally found a bunch
of files
under
C:\Documents and Settings\problemuser\Application
Data\Microsoft\Protect
in
one of the directories. The directory was created at the time
the data
was
pushed to the problem target system. In my case, it contained
over
16,000
files. I moved the new directory out of the Protect directory
to
eliminate
the CPU hit after logon.