

Re: lsass.exe brings machine to its knees.....

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2003-12/1375.html>

From: Cal (*anonymous_at_discussions.microsoft.com*)

Date: 12/20/03

Date: Fri, 19 Dec 2003 15:05:57 -0800

Hi Dave,

I made a set of rescue disks from (updated) AVG and booted the machine in safe mode, then ran it (it runs in a dos window...). No viruses detected. Any possibility that the disks are infected? Also tried to do an online scan at McAfee...but it was so slow that it'd have taken me til '05 to complete it.

I'm not opposed to going out and buying AV software... How sure are you that this is a virus?? Which "flavor" would you recommend? We use Norton corporate at work, and I'm NOT a fan...

Thanks again for all your help!!!!!!

Cal

---Original Message-----

>Go into Safe Mode and perform a full scan of your platform and clean/delete infected files

>as needed.

>

>Dave

>

>

>

>"Cal" <anonymous@discussions.microsoft.com> wrote in message

>news:053901c3c5af\$0ad31460\$a101280a@phx.gbl...

>| JT,

>| I checked the registry per Symatec, and I don't see

>| lsass.exe in a "run" key.... Also ran the system file

>| checker and it didn't find any issues.

>| re: corruption/defrag....I haven't defragged in a

>| while...disk was too full, so last night I deleded a

Re: lsass.exe brings machine to its knees.....

bunch

>| of stuff and ran a defrag. Doesn't seem to have fazed
it

>| a bit. lsass is still hogging the cpu. Any other help

>| you can give me will be GREATLY appreciated!!!

>|

>| Cal

>|

>| >-----Original Message-----

>| ><http://www.blackviper.com/WIN2K/servicecfg.htm>

>| >

>| >lsass.exe handles the IPSEC Policy Agent, Net Logon,

NTM

>| Security

>| >Provider, Security Accounts Manager, and the Kerberos

Key

>| Distribution

>| >Center. (.)The latter is only available on the W2K

>| server.) It isn't a

>| >virus and doesn't get infected with any known viruses

>| (cross

>| >fingers!). However, the Backdoor.IRC.Aladinz.E trojan

>| creates its own

>| >lsass.exe. See:

>| >

>| >

>|

>| ><http://securityresponse.symantec.com/avcenter/venc/data/ba>

>| >ckdoor.irc.aladinz.e.html

>| >

>| >and read the tech details section.

>| >

>| >In some cases where lsass hogged the cpu, it turned out

>| that a

>| >corrupted file existed on the machine and defrag ran in

>| an attempt to

>| >fix it. lsass and defrag were trying to access the same

>| file at the

>| >same time, sending eachother into a loop. go figure.

>| >

>| >

>| >JT

>| >

>| >>><anonymous@discussions.microsoft.com> wrote in
message

>| >>>news:048f01c3c449\$606e3d80\$a501280a@phx.gbl...

>| >>>| this is crazy...I boot my Win2k machine and it runs

>| >>>fine.

>| >>>| I'm at SP4. The minute I log onto my ISP (dialup)

>| >>>| lsass.exe starts consuming 95-100% of my cpu cycles

>| >>>| according to taskman, and brings my machine to its

microsoft.public.security.virus: Re: lsass.exe brings machine to its knees.....

>/>>>/ *knees.... I can log off the net, but lsass.exe
still*

>/>>*hogs*

>/>>>/ *my machine until I shut it down and reboot. Any*

>/>>*ideas????*

>/>>>/ *THANKS*

>/>

>/>.

>/>

>

>

>.

>