

Need help with NTAP32SMS.EXE Virus– ASAP – Mission Critical

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2005-04/0449.html>

From: Craig n (noway_at_getmyemail.com)

Date: 04/27/05

Date: Wed, 27 Apr 2005 09:41:18 -0500

I have a virus hosing one of my critical servers, and it had also nailed my laptop. Symptoms are 99% processor usage, and loss of internet connectivity. I was able to remove it from my laptop, which has XP SP2, and all the security updates, along with Norton AV. Now a server appears to be infected, and it is a 2000 server with mcafee. At first, mcafee was taxing the processor at 99%, stuck in a starting mode, and this morning found that ntap32sms.exe was running on it.

I cant find ANYTHING regarding this process, except I can google ntap32.exe and get back trojan info. AV wont pick it up, so I assume this is new. Does anyone have any info on this?

Also, picking processes called msdirectx.sys, and nviload32.

Oh, and after I remove the files from system32 and prefetch, and destroy the registry entries, they are right back the next boot. Where is it coming from?