

## Re: Multiple Accounts Being Locked Out – HELP Please!!

*Source:* <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2005-01/1145.html>

---

*From:* Steven L Umbach (*n9rou\_at\_nospam-comcast.net*)

*Date:* 01/27/05

Date: Thu, 27 Jan 2005 00:10:16 -0600

My guess is that those computers are infected with something. I would try a different antivirus program for another opinion and make sure you virus definitions are current as of today from your publisher's website.. Trend Micro has the free Sysclean. You just download it and it's pattern file to a folder to run. It will detect and remove many common malwares and generate a report..

<http://www.trendmicro.com/download/dcs.asp> -- read Sysclean.txt for special instructions for NT4.0

<http://www.trendmicro.com/download/pattern.asp>

Also what you can do is to try and investigate further on your own. From SysInternals download Filemon, PsList [part of pstools] TCPView, Autoruns, and Process Explorer. Install them on the problem computers, preferably on an isolated network and use them to check port to process mappings, processes running, and startup programs. Filemon will show file activity in real time and may help you isolate the files causing this. When looking at processes and ports, look for any unusual ports and processes being used and whether or not they are associated with a publishers name – malware usually shows no publisher name and may have a strange filename associated with it, though many times the filename will try to look like something "official". It will help if you can compare processes to a like configured system, ideally a known clean install as you could end up comparing to another infected computer. If you find any rouge processes and executables be sure to contact your antivirus vendor with this information.

Another thing to try would be to install a software firewall on the problem computers and wait for the offending process to pop up a message from the firewall asking your permission to access the network. Keep in mind that "root kit" infections are going around and can be extremely difficult to detect and will evade most host based antivirus scans. The SysInternals tools may expose a rootkit showing additional processes compared to what you see with Task Manager. Alternatively you could use pslist to examine what processes are found locally and then do the same from a remote computer to compare the results. if you want a great resource on learning about malware and how to deal with them download the free Anti Virus in Depth Guide from

microsoft.public.security: Re: Multiple Accounts Being Locked Out – HELP Please!!

Microsoft. The links below may help.

<http://www.sysinternals.com/ntw2k/source/tcpview.shtml> --- TCPview and link to other SysInternals tools – select utilities in upper left hand column.

[http://www.microsoft.com/technet/security/guidance/avdind\\_0.mspx](http://www.microsoft.com/technet/security/guidance/avdind_0.mspx) --- Antivirus in Depth Guide

"JerryAMWE" <JerryAMWE@discussions.microsoft.com> wrote in message news:1156DCF5-9E93-4383-A31E-3E50B9098AFC@microsoft.com...

>I am running a Windows NT 4.0 Domain with a PDC and BDC. We have about 800  
> users. What I noticed today is that each account is being alphabetically  
> locked out because there are a lot of unsuccessful logon attempts (approx.  
> 100 attempts per account). I noticed that the attacks were coming from 3  
> PCs. I removed the PCs from the network and checked to verify that the  
> eventlogs on the PDC/BDC had stopped locking out accounts. About 30  
> minutes  
> later, the problem started again from a different PC. The PCs I had  
> removed  
> were checked for spyware and viruses. One had the Bat.Noshare.v virus,  
> the  
> other was clean. The 4th PC that started causing the problem was also  
> checked for viruses and spyware. It was also updated with critical  
> patches,  
> yet the problem persists. Please help!! I can't determine what is  
> causing  
> this and therefore, I can't find a fix for it.  
>  
> Sincerely,  
> Jerry (At My Witts End)