

Win2000 AD user account mass lockout – Strange !

Source:

http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.active_directory/2004-06/2165.html

From: Dan Sime (*dansime_at_hotmail.com*)

Date: 06/23/04

Date: Wed, 23 Jun 2004 10:47:04 -0700

Hi

On the face of it, it appears you have a virus problem or security problem on that laptop. I know this may appear to be an obvious comment. A few things that might help discover 'how' it happened could be things like:

- > *Is there a firewall in place?*
- > *Are there any abnormal processes running in task manager?*
- > *Does the laptop connect to the internet through anything other than your network? (i.e. is it using it's own connection to the internet, providing an 'un-protected' route into your network from the outside.*
- > *Have you checked Anti-Virus provider websites for info on Viruses that do this?*

Sorry that these are perhaps obvious questions, but those are the areas I would research to get an idea of 'How'.

Probably not much help, but just my thoughts on it.

Cheers

Dan

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

>Very strange – We had a mass lockout of every user account in AD

>yesterday. It was traced to a laptop running WinXP-SPI.

>

>A check of the Security log on the DC shows about 3000 failure audits

>over a 2 minute period, at least 10 per user account. It has somehow

>>walked the AD tree as it's tried everything across

microsoft.public.win2000.active_directory: Win2000 AD user account mass lockout – Strange !

multiple OU's

>including disabled user accounts.

>

>The laptop is running Symantec Antivirus Corporate 8.1

with

>definitions from June 9th.

>

>Anyone ever seen anything like this?

>

>Event Log Sample

>=====

>

>

>Event Type: Failure Audit

>Event Source: Security

>Event Category: Logon/Logoff

>Event ID: 539

>Date: 6/22/2004

>Time: 12:07:02 PM

>User: NT AUTHORITY\SYSTEM

>Computer: xxxxxx-x

>Description:

>Logon Failure:

>Reason: Account locked out

>User Name: joeuser

>Domain: VENTURI-SA5BUXB

>Logon Type: 3

>Logon Process: NtLmSsp

>Authentication Package: NTLM

>Workstation Name: VENTURI-SA5BUXB

>.

>