

Re: Help Me Resolve Event Errors

Source:

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2004-04/5928.html>

From: Malke (*malke_at_nospoonnotreally.com*)

Date: 04/06/04

Date: Tue, 06 Apr 2004 06:21:46 -0700

JD wrote:

- > *We've established a user account for my wife. She has no problems*
- > *logging on or performing any tasks.*
- > *The problem is that each time she logs on, the Event Log records*
- > *numerous "errors."*
- > *The MSKB article says this applies to Windows XP Pro. But this is*
- > *definitely XP Home Edition.*
- > *Here's what I read in the error report returned from Microsoft. I*
- > *especially call attention to the penultimate paragraph. I hope someone*
- > *can explain it and suggest a way to stop this from happening:*
- >
- > *Windows Operating System*
- > *ID: 529*
- > *Source: Security*
- > *Version: 5.0*
- > *Component: Security Event Log*
- > *Symbolic Name: SE_AUDITID_UNKNOWN_USER_OR_PWD*
- > *Message: Logon Failure:*
- > *Reason: Unknown user name or bad password*
- > *User Name: %1*
- > *Domain: %2*
- > *Logon Type: %3*
- > *Logon Process: %4*
- > *Authentication Package: %5*
- > *Workstation Name: %6*
- > *Explanation*
- > *This event record indicates an attempt to log on using an unknown user*
- > *account or a valid user account but with an incorrect password.*
- > *An unexpected increase in the number of these audits could represent*
- > *an attempt by someone to find user accounts and passwords (such as a*
- > *"dictionary" attack, in which a list of words is used by a program to*
- > *attempt entry).*
- >
- > *With the welcome screen and logon/logoff and/or account logon success*
- > *and failure auditing are enabled, pairs of Logon/Logoff failure or*
- > *Account Logon failure audits with successful logon audit entries are*

> *added to the computer security log.*

> *From your description of the problem, it sounds like you have an active trojan on the system or some nasty malware in her account. What does a scan with a current antivirus program (meaning a version not earlier than 2002 and using updated virus definitions) show? Also, remove spyware with Spybot Search & Destroy from www.security.kolla.de and Ad-aware from www.lavasoftusa.com. Be sure to update these programs before running them. It is best to run antivirus and spyware removal tools in Safe Mode.*

Malke

--

MS-MVP Windows User/Shell
Elephant Boy Computers
www.elephantboycomputers.com
"Don't Panic"