

## Re: Is there malware on my Server?

---

*Source:*

<http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2008-04/msg00085.html>

---

- *From:* "Anthony [MVP]" <[anthony@xxxxxxxxxxxxx](mailto:anthony@xxxxxxxxxxxxx)>
  - *Date:* Sat, 26 Apr 2008 15:54:45 +0100
- 

John,

I was looking to see where the Windows authentication failure might have come from. "Administrador" is a failed login attempt, which means you must be exposing to the internet some means of authenticating to the server. It is normal to have failed logon attempts like this when you expose an authenticated service.

You may want to read up on the IIS Security documentation, which is quite good:

<http://technet2.microsoft.com/windowsserver/en/library/ace052a0-a713-423e-8e8c-4bf198f597b81033.mspx?mfr=tr>

Hope that helps,

Anthony

<http://www.airdesk.co.uk>

"John Kotuby" <[jkotuby75@xxxxxxxxxxxxx](mailto:jkotuby75@xxxxxxxxxxxxx)> wrote in message  
[news:OsFsZ\\$upIHA.4292@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:OsFsZ$upIHA.4292@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx)

Anthony (and Meinolf),

Thanks for the response. The consensus seems to be that I must rebuild the server from scratch. Wow, what an endeavor, considering the server is on the other end of the USA about 3000 miles away and I would have to pay the ISP for that time as well as considerable time to set up domains, DNS, etc. myself.

With all that considered it may be time to make the move to a managed hosting environment with a more robust database server. Then the new Hosting company would do the setup and I would need to re-publish the databases and the web applications.

About your question...How are you authenticating the web site?

In IIS Manager, Anonymous Access is checked and the login uses the IUSER\_SITENAME\_ORG and whatever password was assigned by default. Also Integrated Windows Authentication is checked. I never considered those options. I write the code that makes the application work, including the

Re: Is there malware on my Server?

database access (which is mixed but uses SQL Server login from within the application itself).

When a user surfs to the site, anyone is allowed to the "Login Page" but if a validated UserID and PassWord is not entered the user can go no further. I use SQL Server to store user logins and passwords.

When we do "re-make" the server, do you suggest a different form of web site authentication? I am presuming you are referring to the settings in IIS Manager.

Thanks

"Anthony [MVP]" <anthony@xxxxxxxxxxxx> wrote in message [news:erwkMeXpIHA.1768@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:erwkMeXpIHA.1768@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

I am sorry but if your computer was hacked you really have to start again. You must have a firewall, and that must block any connections except over http, https etc.

Administrador indicates hack attempts to log on with the Administrator account using NTLM.

How are you authenticating the web site?

Anthony,

<http://www.airdesk.com>

"John Kotuby" <jkotuby75@xxxxxxxxxxxx> wrote in message [news:Oe\\$G4GXpIHA.3428@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:Oe$G4GXpIHA.3428@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

In the event log under Security, on our remote leased dedicated Web Server I have just noticed multiple failed logon attempts that go back about 3 weeks. They are all like the one I am showing below:

Date: 04/23/2008 Source: Security  
Time: 10:02:34 AM Category: Account logon  
Type: Failure Aud Event ID: 680  
User: NT AUTHORITY\SYSTEM  
Computer: LUNARPAG-SEOGSA

Logon attempt by:  
MICROSOFT\_AUTHENTICATION\_PACKAGE\_V1\_0  
Logon account: administrador  
Source Workstation: TMYFREE5005  
Error Code: 0xC0000064

Other error codes have been 0xc000006A.

At first I thought it was the hosting company support staff

Re: Is there malware on my Server?

trying to  
log onto our server. But they replied that since we don't have  
"managed  
hosting" it would not be their staff and it is probably a  
hacker. Well  
that is very disconcerting. I told them it looked like the  
attacks were  
coming from within their network because no "remote  
service" appears to  
be mentioned in any of the failure details. They all come  
from the  
SYSTEM account and the Source Workstation name keeps  
changing, although  
I have seen some repeats.

Now upon closer inspection, it seems as if maybe the attacks  
are  
originating from the Server itself...that is just a guess.

I have disabled the Administrator account.  
About 3 months ago we were compromised by a hacker from  
South Vietnam. I  
thought I cleaned all the junk that was left from that attack.  
Maybe  
that is not the case.  
At that time I disallowed Terminal Server connections by  
Administrator  
account and changed the password.

Can anyone shed some light on this behavior? I am not a  
network  
administrator and I am having trouble getting help from the  
hosting  
company. Yes I am looking to change Hosting companies,  
but that would  
require a lot of time and I have prospective customers  
looking at our  
very large ASP.NET application starting tomorrow.

Is there any way that I might track down the real source of  
these logon  
attempts?

Help...

Any input would be appreciated.

Re: Is there malware on my Server?