

Re: Login Errors Seem to indicate we are being hacked?

## Re: Login Errors Seem to indicate we are being hacked?

---

*Source:*

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2008-09/msg01116.html>

---

- *From:* Siv <[Siv@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:Siv@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Sat, 13 Sep 2008 12:57:00 -0700
- 

Teneo,

Many thanks, that explains it. They have a wireless network as well as the wired LAN and I was wondering if the logins were coming through that. It's protected with WPA2 and strong Key so I would be surprised if that was getting compromised.

I'll turn on the logging and complain to their ISP's Abuse team.

Thanks for your help.

Siv

—

Martley, Near Worcester, UK

"Teneo" wrote:

Hi Siv, the key here is MICROSOFT\_AUTHENTICATION\_PACKAGE\_V1\_0

This is an attempt on your email / port 25 system, use you as a relay.

Switch on SMTP logging and in the logs you will find the IP to block if you wish to investigate.

Hope it helps

"Siv" <[Siv@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:Siv@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)> wrote in message  
<news:60D337F0-493E-443E-88B1-116ADF2BB5D8@xxxxxxxxxxxxxxxxxxxx>

Hi,

In the logs this morning for one of my clients I have had about 500 failed logins in teh Security logs. I looked at the Security Event Log and filtered for failures and there were hundreds of attempts in very quick succession

Re: Login Errors Seem to indicate we are being hacked?

Re: Login Errors Seem to indicate we are being hacked?

some using the same user name (and presumably different passwords) and then loads of different user names one after the other which sounds like a brute force attempt to gain access.

We use very strong passwords so I am not worried they will have got in, but I would like to ascertain how they were doing it as no IP addresses were quoted so they weren't getting in via the net (unless they were somehow hiding their IP Address). The typical log entry looks like this:

Event Type: Failure Audit  
Event Source: Security  
Event Category: Logon/Logoff  
Event ID: 529  
Date: 12/09/2008  
Time: 12:29:41  
User: NT AUTHORITY\SYSTEM  
Computer: SERVER01  
Description:  
Logon Failure:  
Reason: Unknown user name or bad password  
User Name: pentium  
Domain:  
Logon Type: 3  
Logon Process: Advapi  
Authentication Package:  
MICROSOFT\_AUTHENTICATION\_PACKAGE\_V1\_0  
Workstation Name: SERVER01  
Caller User Name: SERVER01\$\br/>Caller Domain: MOUNTAINASH  
Caller Logon ID: (0x0,0x3E7)  
Caller Process ID: 1692  
Transited Services: –  
Source Network Address: –  
Source Port: –

For more information, see Help and Support Center at <http://go.microsoft.com/fwlink/events.asp>.

How do you interrogate the above entry into a meaningful explanation of how they were logging in. Ie what is a logon type 3 and what do the caller Login ID and Process ID tell me??

Any help appreciated.

Siv

Re: Login Errors Seem to indicate we are being hacked?

—  
Martley, Near Worcester, UK