

Re: DNS pointing to porn site

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.dns/2006-01/msg00422.html>

- *From:* "Herb Martin" <news@xxxxxxxxxxxxxxxx>
 - *Date:* Tue, 24 Jan 2006 23:03:32 -0600
-

"GJB" <gjb@xxxxxxx> wrote in message
news:uwZiVSOIGHA.3460@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

> Herb,

>

> Thank for the reply. I can rule out 1 and 2, and have spoken to the
> Manager of the DNS servers we forward to and they aren't compromised, so I
> guess it is "out there" in the wider web-world. I am surprised that there
> is nothing on the grapevine about it if that is the case.

>

It is almost certainly coming from some local or internal
problem in your systems — either client side or DNS Server
side.

If you are taking the "Manager of DNS"s word then you haven't
tested it yourself.

Use NSlookup and other tools to find out WHERE the answer
is originating.

Based on what you have said, I doubt you have even eliminated
the client side.

Have you explicitly tried pings vs. nslookup (to see if you get
the same answers)? A hosts file won't be used by NSlookup.
Also, using explicit DNS servers (working through EACH that
can be involved) until you locate which one(s) return the wrong
info.

You can use (sparingly and politely) 4.2.2.1 and my own
68.178.144.60 as public DNS servers (for comparison) or
to get ROOT server and COM (etc) server addresses for
direct query (to see if you internal servers used the same
server sets etc.)

Remember to be gentle when you use someone else's servers
for such testing.

Re: DNS pointing to porn site

--
Herb Martin, MCSE, MVP
Accelerated MCSE
<http://www.LearnQuick.Com>
[phone number on web site]

> Gerry.
>
>
> "Herb Martin" <news@xxxxxxxxxxxxxxxx> wrote in message
> [news:%23AfWZ\\$PIGHA.604@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:%23AfWZ$PIGHA.604@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)
>> "GJB" <gjb@xxxxxxx> wrote in message
>> news:%23dPe0qPIGHA.648@xxxxxxxxxxxxxxxxxxxxxxxxxxxx
>>> Hi,
>>>
>>> For a day or so we have been having an intermittent problem where users
>>> attempting to access "normal" web site e.g My Ebay, Firstchoice, AOL,
>>> BBC etc have been directed to a porn site www.rug-munchers.com.
>>> Has anyone seen this or anything info related to it?
>>>
>>
>> Well, "seen it"? In a way, it means your clients are using
>> a DNS server that resolves it that way either directly or
>> indirectory (unless this is due to some local virus/trojan
>> on the clients, including a modification of the hosts files.)
>>
>> The key is to find WHERE the incorrect data is originating:
>>
>> 1) Clients
>> 2) Local DNS server
>> 3) Forwarder
>> 4) etc.
>>
>>
>> --
>> Herb Martin, MCSE, MVP
>> Accelerated MCSE
>> <http://www.LearnQuick.Com>
>> [phone number on web site]
>>
>>
>
>

-
- *References:*
 - ◆ [DNS pointing to porn site](#)

Re: DNS pointing to porn site

◇ *From:* GJB

◆ ***Re: DNS pointing to porn site***

◇ *From:* Herb Martin

◆ ***Re: DNS pointing to porn site***

◇ *From:* GJB

- Prev by Date: ***Re: DNS pointing to porn site***
- Next by Date: ***Re: AD integrated DNS transfer***
- Previous by thread: ***Re: DNS pointing to porn site***
- Next by thread: ***Re: DNS pointing to porn site***
- Index(es):
 - ◆ ***Date***
 - ◆ ***Thread***