

Re: DNS cache corruption

Source:

<http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.dns/2005-04/msg00113.html>

- *From:* "Kevin Nickell" <knickell@xxxxxxxxxxx>
 - *Date:* Tue, 05 Apr 2005 16:15:13 GMT
-

Thanks. I will try that. Microsoft also has us running a bunch of kernel scanners to see if the local machine has been compromised. No Spyware, Adware or viral activity is found. Nothing in any task scheduler. No unknown processes or services running....

Wierd.

Kevin

"Brian S. Bergin" <net.terabyte@xxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:aku451tkceg2eroef6hte8clvtkgelaimc@xxxxxxxxxxx

> "Microsoft support" <knickell@xxxxxxxxxxx> wrote:

>

>>I have a horribly confusing problem. Have a client who three times in the
>>last week has had every entry in their DNS cache on a windows 2000 server
>>set to the same IP address. The address, all three times, resolves to
>>www.jothan.com. Every website not resolved directly by the internal DNS
>>server redirects to jothan.com. The reason I worry about this is that
>>this

>>is a site run by Jothan Frakes who is a DNS TLD expert influential with
>>ICANN. If I simply clear the DNS cache, it is not fixed and the cache
>>sets

>>every entry back to the ip of www.jothan.com. If I restart the DNS
>>server,

>>then clear the cache it is fine for a day or so.

>>

>>The second worry I have is that this issue started first thing the morning
>>of April fools day.

>>

>>Anyone with any idea whatsoever? They are using root hints and we
>>switched

>>to forwarders, just in case.

>>

>>Kevin Nickell

>>

>

> Have you enabled DNS Cache Pollution protection? In the DNS MMC,
> right click on the server name, Properties, Advanced, "Secure Against

Re: DNS cache corruption

> DNS Cache Pollution".
>
> Sincerely,
> Brian S. Bergin
> Terabyte Computers, Inc.
>
> Please post replies here so everyone may benefit.
>
> NOTICE: Use of this information is contingent upon acceptance of Paragraph
> 17 of Terabyte's Terms and conditions located at
> <http://terabyte.net/terms.htm#postings>.

• *Follow-Ups:*

- ◆ **Re: DNS cache corruption (poisoning)**
 ◇ From: bntjnk

• *References:*

- ◆ **DNS cache corruption**
 ◇ From: Microsoft support
- ◆ **Re: DNS cache corruption**
 ◇ From: Brian S . Bergin

- Prev by Date: **Re: DNS issue**
- Next by Date: **Re: Dns problem seeing the domain**
- Previous by thread: **Re: DNS cache corruption**
- Next by thread: **Re: DNS cache corruption (poisoning)**
- Index(es):
 - ◆ **Date**
 - ◆ **Thread**