

Re: Was this poisoning, spoofnig, or something else?

## Re: Was this poisoning, spoofnig, or something else?

---

*Source:*

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.dns/2007-12/msg00160.html>

---

- *From:* "Kevin D. Goodknecht Sr. [MVP]" <[admin@xxxxxxxxxxxxxxxx](mailto:admin@xxxxxxxxxxxxxxxx)>
  - *Date:* Sun, 16 Dec 2007 15:04:09 -0600
- 

Read inline please.

In <news:MPG.21cf7af7a4b63e499898bd@xxxxxxxxxxxxxxxxxxxxxxxx>,  
Thorsten Kampe <[thorsten@xxxxxxxxxxxxxxxx](mailto:thorsten@xxxxxxxxxxxxxxxx)> typed:

- \* Kevin D. Goodknecht Sr. [MVP] (Sat, 15 Dec 2007 23:03:06 -0600)  
[snipping all the previous stuff because it got too long]

Nslookup uses the DNS client's DNS suffix search list, it does NOT always devolve the name, you should test it yourself, I have.  
If the DNS client has only one suffix in the search list, no matter how may levels the suffix is, it will append only the suffix(es) in the list..

Sorry, you now see me confused: Steve's problem was that he discovered that all queries like "nslookup www.test.com" returned "www.test.com.test.com (china address)".

I replied that he's got two issues. One is his incorrect nslookup query – he simply forgot the trailing point, so automatically his local domain was added. His local DNS forwards the query to his ISP's DNS because the local DNS is authoritative for test.com but not for test.com.test.com.

If his local DNS server is Authoritative for test.com, explain why you think it would not have Authority for test.com.test.com?

The second is (and here I cannot be one hundred percent sure but it's by far the most likely explanation) his ISP's DNS does a "catch all" for unknown domains and therefore responded with a wrong reply. So this forwarder's cache was likely poisoned (and not the local one's).

Re: Was this poisoning, spoofnig, or something else?

Re: Was this poisoning, spoofnig, or something else?

If his ISP did a "catch all" (Wildcard) for all unknown domains, how would anyone using that ISP be able to resolve any domain name?

After all, I highly doubt that the ISP's resolving DNS proxy is authoritative for any domains, much less all known domains, so every domain would hit the wildcard. Wildcard records should only exist in Authoritative servers.

So neither "DNS suffix search list devolution" (what ever that may be) or "a wildcard record in the public domain 'test.com'" or "internal DNS not authoritative for test.com", or "external IP in his DNS servers list" or "does not have a zone for his internal Domain in his local DNS server" have anything to do with Steve's problem.

Any or all of these would or could be the problem. I guess we'll never know since Steve has not responded in this group, since he made his original post.

--

Best regards,  
Kevin D. Goodknecht Sr. [MVP]  
Hope This Helps

=====  
When responding to posts, please "Reply to Group" via your newsreader so that others may learn and benefit from your issue, to respond directly to me remove the nospam. from my email address.

=====  
<http://www.lonestaramerica.com/>  
<http://support.wftx.us/>  
<http://message.wftx.us/>

=====  
Use Outlook Express?... Get OE\_Quotefix:  
It will strip signature out and more  
<http://home.in.tum.de/~jain/software/oe-quotefix/>

=====  
Keep a back up of your OE settings and folders with OEBackup:  
<http://www.oehelp.com/OEBackup/Default.aspx>

.

Re: Was this poisoning, spoofnig, or something else?