

# RE: ExcludeNodes setting bypassed

*twinkletoedturtle*

Fri, 12 Feb 2010 03:10:20 -0800

This thread is being forked from the original as it doesn't entirely depend on the user(s) using bridges and this problem. I understand the purpose of Tor and know individuals, organizations, as well as governments use Tor, so why be surprised when governments use Tor? But if these individuals are correct, why are dc nodes making the exception with ExcludeNodes and passing through? Is there an attack on Tor certain nodes use to bypass this feature?

From: Andrew Lewman

"Yes, https://bugs.torproject.org/flyspray/index.php?do=details&id=1090.
 We're still working on it.  In fact, we're working on rewriting the entire codebase around {Exclude}{Entry|Exit}Nodes options."

Thanks. May I ask when this bug was first noted? I've only come across it in the most recent version of Tor. How is it it's a bug when it openly tells you it's going ahead without your permission to use a node in exclusion? This would not appear as a bug to me, maybe I'm wrong. Myself and others have noticed this excludenodes function often allows specific nodes to pass through with the warning, normally nodes labeled as washdc nodes.

I'd like to quote from an .onion discussion on this subject, as several people there feel comfortable posting anonymously but may not wish to post in public here.

Here are some comments from anonymous users:

ExcludeNodes Is Useless And Flawed
- Read The Reply From A Tor Developer
http://l6nvqsqivhrunqvs.onion/?do=topic&id=9974

"I'm not surprised. They should post more about what they're really working on in Tor, such as the bug you mentioned, which I bet most didn't know of until now, on their precious blog: https://blog.torproject.org instead of their usual
version releases. What's next for the users to find?"

"# Is this a bug?
#
#Yes

LOL, right, how could it possibly be a bug when the function and response to the user is printed out? Was this a gem cleverly inserted into the new version of Tor? I wouldn't be the bit surprised, especially this following the offensive and virus like "bloxor" nodes discussed on these forums and at the Tor mailing list.

Or, maybe, just maybe, the washdc and amazon nodes, along with the 149.* nodes were tired of being blocked. "

"You guys don't read your Onionforum regularly! I've posted about this months ago, several times in fact. The behaviour I noticed was that it didn't happen with ALL nodes, only some seemed to plow right on through the Exclude

condition
(namely those Washington DC "mystery" nodes - long suspected of being LEA's
own
or perhaps even NSA spy nodes).
Second, how can this be a bug? How hard is it to write the C code that says
"if
that node's name is listed in the config, don't use it". It's put forth like
some massively complex problem requiring a full re-write of the Tor code, but
it's not.
Maybe it's just CALEA for Tor... "

"I concur, ExcludeNodes function is useless as of Tor v0.2.1.22. Something has
been added
to negate the ExcludeNodes function, this has never happened to my Tor usage
prior to
this version.

Try this with your torrc file and the ExcludeNodes option:

1. block all nodes used by your ISP (excluding your own, assuming you're
running as a client only)
2. block all washdc nodes
3. bloack all amazon nodes
4. block all 149.* nodes
5. block all "bloxor" nodes (see related thread on these forums about "bloxor"
nodes)

Now, use Tor as a client for a few hours, browsing as you normally do, watch
your tor logs and
note the message: (where X = nodename and # = numerical value)

[warn] Requested exit node 'X' is in ExcludeNodes or ExcludeExitNodes.
Using anyway (circuit purpose #).

I've also seen:

[warn] exit circ (length #, exit *X*)

I'm certain the Tor project is probably useless for privacy now when it's
over riding user's configuration policies. It was good while it lasted.

Should anyone pick through the code and discover how to disable this

privacy violation, please post here. "

"It never worked.

But there are more flaws. Think about a path like this:

entry:{us} -> middel:{us} -> exit:{us} all in the same country.
entry:{us} -> middle:{??} -> exit:{us} what ? same problem.

That happens randomly very often.."

Confirmed exclude nodes not effective for me as well. I've got nixnix and jalopy in my online relays list (they're supposed to be exluded so shouldn't show up) and I've just used a node that's supposed to be excluded from Estonia. Has anyone else had nodes not excluded that aren't from the US? (mainly referring of course to those DC nodes)"

[ Another thread which references this oddity: ]

Tor Trapdoors? How To Trigger Them
- try this and see if you can duplicate it
http://l6nvqsqivhrunqvs.onion/?do=topic&id=9854
**********
To unsubscribe, send an e-mail to majord...@torproject.org with unsubscribe or-talk in the body. http://archives.seul.org/or/talk/


- **RE: ExcludeNodes setting bypassed** *twinkletoedturtle*
  - **Re: ExcludeNodes setting bypassed** *Nick Mathewson*
    - **Re: ExcludeNodes setting bypassed** *G-Lo* •
  - **Re: ExcludeNodes setting bypassed** *Scott Bennett*

twinkletoedturtle