or-talk

Thread Date

Search

Re: ExcludeNodes setting bypassed

Nick Mathewson

Fri, 12 Feb 2010 19:29:08 -0800

```
On Fri, Feb 12, 2010 at 6:10 AM,  <twinkletoedtur...@safe-mail.net> wrote:
> 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."

I'll try to expand on the understand the bug report you are citing, since the stuff there really _does_ explain what the problem is, albeit in programmer-speak.

The root problem here is in the way that node selection was originally written. We needed to solve the question of, "what should we do when the user requests that only certain nodes be used, and then makes a request that those nodes cannot satisfy?" Some examples where excluding nodes can make it impossible to fulfill a request include:

- Excluding a node, then choosing that node as the exit for a particular circuit.
- Excluding every introduction point for a hidden service, then trying to connect to that hidden service.
- Excluding every distributed directory point for a hidden service, then trying to look up its descriptor.
- Operating a hidden service, when the client picks a rendezvous point you've excluded.
- Trying to connect to an IP:Port when you have excluded every exit node that would support it.
- Trying to bootstrap when you have excluded every directory authority.

In *most* of these cases, we figured that recent requests should override old requests, so if the user says "don't do X" and then says "do X", they probably meant the latter rather than the former. Similarly, we figured that people mostly wanted their requests not to break, and would get irritated if excluding nodes meant that their hidden service requests could break at random. So (IIUC) we set up the code so that some service requests that could only be granted with excluded nodes would produce a warning rather than a complete failure.

It turns out this wasn't the choice a lot of people want: they want to be able to say "Never ever ever use these nodes. If I ever make a request that can only be satisfied with nodes I've excluded, reject that request, even if it means I don't get the hidden services I want, or I can't bootstrap, or whatever." This isn't a crazy thing to ask for at all. As Andrew said, Roger's working on rewriting big chunks of the node selection code to support this feature. As Andrew said, check out Bug 1090 for the details and progress.

(Another confusing aspect here is that "exclude X as an exit node" has been taken by some people to mean that all circuits ending at X should be verboten. But circuits can end at a node for reasons other than sending traffic out of the network, including accessing a hidden service via a rendezvous point, performing a self-test, or accessing a directory server. Perhaps what people really want is an ExcludeAsLastHop option, and we should build that instead.)

Another goal of the node-selection rewrite, BTW, is to simplify the node selection process. It's pretty complex, and there could well be more bugs in it. We should also work on specifying the whole thing better, so it's easier to tell surprises from bugs; Sebastian said he was interested in trying that out in whatever free time he has left.

So that's what's going on here. It is not in fact, a sooper-sekrit government backdoor. There is not any exception for nodes in Washington, Moscow, Area 51, or the Bermuda Triangle. It's a node selection algorithm which was originally written with a false UI assumption (that people would want working requests to trump configuration settings), and which Roger's been trying to make more like what people want. Some of it's already rewritten in 0.2.2.x; some will take more work.

And as for whoever thinks that Roger not getting the code rewritten fast enough for their taste means that we're a bunch of contemptible lying double-dealing sellouts who would sabotage our own life's-work for whatever reason: They are mistaken. For my part, I'd rather quit software entirely than back-door Tor, and I believe that goes for everybody on the project.

Sorry for the intemperate digression.

Hope this helps,
--
Nick

```
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*

Reply via email to

Nick Mathewson