

[Full-disclosure] Major ISPs arbitrarily blocking IRC and hijacking DNS entries

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2007-07/msg00394.html>

- *From:* Anthony <anthony@xxxxxxxxxxx>
 - *Date:* Thu, 19 Jul 2007 00:05:04 -0400 (EDT)
-

Greetings:

I am writing to this list because I no longer know where to turn. Over the course of the past 2 to three weeks I have watched my services on the internet become systematically blocked and redirected by no less than 3 major isps in their efforts to stop botnets from connecting to IRC. Allow me to provide a little background info.

My name is Anthony Sanchez and I have run a small irc network, for the past 6 years, along with a couple websites and my mail server (utilized by two people). Approximately 2 weeks ago, we discovered that TimeWarner/Road Runner/AOL was redirecting traffic from irc.ablenet.org port 6667 to their own dummy install of ircd along with commands to connecting users to ".remove" in the event that the connection was a bot. If the end user were to attempt to speak or issue a command, that user was banned from the 'dummy' network.

At about the same time, we noticed that verizon was restricting access to the IPs all together, apparently using some form of port restriction as the DNS still resolved on their name servers correctly. I have documented this informally, with screenshots, on my weblog, found at <http://anthony.blogs.ablenet.org/>.

As of today, it now appears that Cox is also redirecting traffic apparently in an effort to disable botnets.

As you can see below, the correct resolution of irc.ablenet.org is as follows:

Name: irc.ablenet.org
Address: 65.23.156.37
Name: irc.ablenet.org
Address: 65.19.178.15

Contrary to the truth, cox.net resolves it as so:

Server: ns1.dc.cox.net
Address: 68.100.16.30

Name: irc.ablenet.org
Address: 70.168.70.4

Out of concern, I had emailed the irc-unity.org security discussion list (currently cc'd; I hope that is ok) and confirmed that while not everyone is experiencing this problem, it is not entirely new. That being said, I am not sure anyone has experienced it on this level. We have never harbored botnets; in fact, we have very strict connection policies and have flown under the radar for a good number of years.

I assure you all that we have never and will never contribute to the abuse of the internet. A cursory scan of the general blacklists does not appear to show any submission of my IPs or my URL. To make matters worse, we have no means of recourse or correction. No one has made an effort to contact me with regards to their plans and how I may have been able to prevent what amounts to a systematic crippling of services. I have no way to circumnavigate the domain hijacking, port blocking or traffic redirection being employed. Nor do I have any useful contact information that would put me in contact with any of their network security personnel. These providers, while perhaps noble in their cause, are denying us our right to exist. If we were a large organization, this very likely would not be happening.

I appeal to the members of this list and those that read it. If anyone can offer any form of assistance, knows anyone who can, or can help me get my story out... please do. Beyond the inability to exist, I am concerned for the communities that have congregated with us and contributed to the greater good. Any and all assistance will be beyond appreciated, as our very existence is at stake and I no longer know what to do...

Best Regards,
Anthony Sanchez
Anthony at AbleNET dot Org

Full-Disclosure – We believe in it.
Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>
Hosted and sponsored by Secunia – <http://secunia.com/>