

# [PL #25117] DNS Update Attempts

André Martin via RT [support at planet-lab.org](mailto:support@planet-lab.org)

Thu Apr 17 05:49:52 EDT 2008

- Previous message: [\[PL #25117\] DNS Update Attempts](#)
- Next message: [\[PL #25119\] request for role change](#)
- Messages sorted by: [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#)

Email Recipients (see <http://www.planet-lab.org/Support>)

Owner: Nobody

Requestor: [gmc\\_d at pretel.com.au](mailto:gmc_d@pretel.com.au)

Ticket Ccs: [gert.pfeifer at inf.tu-dresden.de](mailto:gert.pfeifer@inf.tu-dresden.de), [gmc\\_d at pretel.com.au](mailto:gmc_d@pretel.com.au), [tudresden\\_sedns at slices.planet-lab.org](mailto:tudresden_sedns@lices.planet-lab.org)

=====

Hi Graham & Sapan,  
we are currently performing a research project concerning content distribution in the DNS name space.  
In order to discover those CDNs, we've developed a crawler/spider system that gathers DNS data through AXFRs (zone transfers) and similar approaches. You can find more information about our research project and team @ <http://wwwse.inf.tu-dresden.de/SEDNS/> AXFRs is the intended behavior of our software that runs on the planet lab nodes.  
If you feel bothered by our DNS crawlers, we can black list your DNS server(s) and/or zone(s) so that you will never find AXFR attempts from our system in your logs again. Let us know!  
Thanks and have a great day.

Cu on the 'net,

Bye - bye,

<<<< André <<<< >>>> èrbnA >>>>

Sapan Bhatia via RT wrote:

> Hello again,

>

> The researchers responsible for this behavior are cc'd. tudresden\_sedns:  
> please explain your experiment.

>

> Sapan

>

>

>> [[gmc\\_d at pretel.com.au](mailto:gmc_d@pretel.com.au) - Wed Apr 16 23:30:28 2008]:

>>

>> Hello Sapan

>>

>> Thanks for your prompt reply.

>>

>> These are the 3 log entries for the attempts. Our time zone is GMT + 8  
>> and the IP of the DNS is 203.23.128.1

>>

>> Apr 15 12:58:56 services01 named[13040]: client 132.239.17.225#47990:  
>> zone transfer 'lzt.com.au/IN' denied

>> Apr 16 03:41:01 services01 named[13040]: client 138.23.204.232#48808:

>> zone transfer 'lzt.com.au/IN' denied

>> Apr 16 03:49:55 services01 named[13040]: client 205.189.33.178#50309:

>> zone transfer 'lzt.com.au/IN' denied

>>

>> I hope this is sufficient for your investigations.

>>

>> Regards

>>

>> Graham McDonald

>>

>> -----Original Message-----

>> From: Sapan Bhatia via RT [[mailto:support at planet-lab.org](mailto:support@planet-lab.org)]

>> Sent: Thursday, 17 April 2008 11:11 AM

>> To: Graham McDonald

>> Subject: [PL #25117] DNS Update Attempts

>>

>> Email Recipients (see <http://www.planet-lab.org/Support>)

>> Owner: Nobody

>> Requestor: [gmc\\_d at pretel.com.au](mailto:gmc_d@pretel.com.au)

>>

>>

>> =====

>>

>> Hello,

>>  
>> PlanetLab (<http://www.planet-lab.org/>) is a distributed systems research  
>> test bed. We manage 700+ machines world wide. These machines may share  
>> access to both research, local and public Internet. These services are  
>> actively managed by researchers granted access to PlanetLab accounts.  
>> And, we enforce a project Acceptable Use Policy (AUP)  
>> <https://www.planet-lab.org/aup> that should direct the behavior of  
>> researchers running experiments within PlanetLab.  
>>  
>> We are very concerned by what you have reported to us. The activity in  
>> your report demonstrates a violation of our AUP, namely probing a single  
>> target machine outside the PlanetLab network from many PlanetLab nodes.  
>>  
>> The traffic you've identified was generated as part of a distributed  
>> active network probing experiment running on PlanetLab.  
>>  
>> Our logs show that there are over 10 users on this system that generate  
>> DNS-related traffic. IN order to single out the researchers that caused  
>> the traffic in question, we'll need some additional information, eg. the  
>> exact time at which this traffic was generated, or the destination IP  
>> address.  
>>  
>> Sapan  
>> PlanetLab Support  
>>  
>>  
>>> [[gmcd at pretel.com.au](mailto:gmcd@pretel.com.au) - Wed Apr 16 22:30:09 2008]:  
>>>  
>>> Yesterday I observed 3 attempts to initiate zone transfers to a DNS  
>>> for the lzt.com.au domain that I administer. Two of the 3 IP addresses  
>>>  
>>> I believe are within the PlanetLab domain whilst the third is unknown.  
>>>  
>>> The IP's are: 138.23.204.232, 205.189.33.17 and 132.239.17.225.  
>>>  
>>> Can you please explain why the zone updates were attempted? If not can  
>>>  
>>> you please investigate the action as it may identify illegal  
>>> activities by someone in your organisation.  
>>>  
>>> Thank you.  
>>>  
>>> Graham McDonald  
>>> Precision Telecommunications Pty. Ltd.  
>>> 134 Burswood Road  
>>> Burswood, Western Australia 6100  
>>> Ph: 61 8 9467 4996  
>>> Fax: 61 8 9470 1313  
>>> Mob: 0418 900 787  
>>> e-mail: [gmcd at pretel.com.au](mailto:gmcd@pretel.com.au)

- 
- Previous message: [\[PL #25117\] DNS Update Attempts](#)
  - Next message: [\[PL #25119\] request for role change](#)
  - Messages sorted by: [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#)

---

[More information about the support-community mailing list](#)