[PL #24064] Re: PlanetLab Traffic Report Feedback - princeton_traffic

Harlan Yu via RT support at planet-lab.org
Thu Feb 14 11:01:27 EST 2008

- Previous message: [PL #24059] planetlab1.tmit.bme.hu - abuse
- Next message: [PL #24059] planetlab1.tmit.bme.hu - abuse
- **Messages sorted by:** [date] [thread] [subject] [author]

```
Email Recipients (see http://www.planet-lab.org/Support)
       Owner: Nobody
       Requestor: zorba at vt.edu
       Ticket Ccs: William at vt.edu, abuse at vt.edu, mkg at vt.edu, rhodes at vt.edu, tml at exchange.vt.edu

================================================

Hi,

This looks like our traffic and not a DNS cache poisoning attack.  We
are running a research experiment to probe DNS caches to try to
estimate the rate of web traffic to different websites.

Bill, I think it's safe to restart your node in normal non-debug mode.

Phil, I will add your server (69.17.112.250) to the blacklist once the
Planetlab node is back up.  We apologize for the packets.

Best,
Harlan.

On Thu, Feb 14, 2008 at 10:45 AM, Bill Marmagas via RT
<support at planet-lab.org> wrote:
> Email Recipients (see http://www.planet-lab.org/Support)
>        Requestor: zorba at vt.edu
>        Ticket Ccs: William at vt.edu, abuse at vt.edu, mkg at vt.edu, rhodes at vt.edu, tml at exchange.vt.edu
>
>  ================================================
>
>  Thu Feb 14 10:45:18 2008: Request 24064 was acted upon.
>  Transaction: Ticket created by zorba at vt.edu
>
>  Subject: Re: PlanetLab Traffic Report Feedback - princeton_traffic
>
>  Since I have not had a response yet, I am rebooting this node into
>  debug state so that it is off-line to researchers but available to
>  Planet-Lab sysadmins to investigate.
>
>
>  On Feb 14, 2008, at 10:31 AM, Bill Marmagas wrote:
>
>  >
>  >
>  > Begin forwarded message:
>  >
>  >> From: PlanetLab Support <support at planet-lab.org>
>  >> Date: February 14, 2008 10:27:44 AM EST
>  >> To: princeton_traffic at slices.planet-lab.org
>  >> Cc: support at planet-lab.org, zorba at vt.edu
>  >
> >> Subject: PlanetLab Traffic Report Feedback - princeton_traffic
>  >> Reply-To: PlanetLab Support <support at planet-lab.org>
>  >
>  >
> >>
>  >>
>  >> PlanetLab Traffic Report Feedback - princeton_traffic
>  >>
>  >> PlanetLab has received feedback from zorba at vt.edu regarding
>  >> the following traffic transmitted by your slice:
>  >>
>  >> Start Time: Feb 13 23:09:14
>  >> End Time: Feb 13 23:59:50
>  >> Slice: princeton_traffic
>  >> Protocol: UDP
>  >> Source IP: bob.cc.vt.edu
>  >> Source Port: n/a
>  >> Destination IP: 69.17.112.250
>  >> Destination Port: domain (53)
>  >> KPackets: 0.91
>  >> KBytes: 55.74
>  >>
>  >> Comments:
>  >> Virginia Tech received the following abuse report that seems to be
>  >> related to your research slice:
>  >>
>  >> ----- Forwarded message from Phil Karn  -----
>  >>
>  >> Date: Wed, 13 Feb 2008 19:17:53 -0800
>  >> From: Phil Karn
>  >> To: benchoff at vt.edu, abuse at vt.edu
>  >> Subject: [ABUSE] Network abuse report
>  >>
>  >> Hi. You are listed as the technical contact in 'whois' for vt.edu.
>  >> I couldn't
>  >> find a specific abuse reporting address listed so I am sending to
>  >> you as well as
>  >> "abuse at vt.edu". If you are not the right person to handle computer
>  >> security
>  >> incidents, please forward this to the correct person.
>  >>
>  >> I am seeing a steady stream of requests to my DNS server from a
>  >> computer at VT.
>  >> The IP address is 198.82.160.221, which resolves back to
>  >> bob.cc.vt.edu.
>  >>
>  >> The queries are for a long list of well known domain names, e.g.,
```

> >> www.yahoo.com
> >> or www.cnn.com. There are far too many kinds of attacks on the
> >> Internet for me
> >> to be familiar with the details of every one, but I suspect this
> >> is a "cache
> >> poisoning" attempt. I.e., if he can find a domain entry already in
> >> my cache, he
> >> can try to replace it with an unsolicited response so that when I
> >> visit that
> >> site again, I can be steered to a different IP address.
> >>
> >> I believe my version of the BIND nameserver is resistant to this
> >> particular
> >> attack; it answers every remote request with an error whether or
> >> not the
> >> requested domain is already in my cache, so his scanning is
> >> pointless. But I
> >> would like to report it anyway as whoever is doing this is
> >> probably attacking
> >> many other systems. You may also wish to examine bob.cc.vt.edu in
> >> case it has
> >> been compromised by a remote party and is being used to launch
> >> these attacks.
> >>
> >> Thanks,
> >>
> >> Phil Karn
> >>
> >> P.S. I have appended a packet trace of a small sample of the
> >> queries. My
> >> apologies for the way lines are wrapped.
> >>
> >> 2:54:55.888977 IP (tos 0x20, ttl 48, id 32520, offset 0, flags
> >> [DF], length:
> >> 59) 198.82.160.221.8582 > 69.17.112.250.53: [udp sum ok] 0 A?
> >> www.yahoo.com. (31)
> >> 02:54:55.890467 IP (tos 0x0, ttl 63, id 0, offset 0, flags [DF],
> >> length: 531)
> >> 69.17.112.250.53 > 198.82.160.221.8582: [udp sum ok] 0- 0/13/14
> >> (503)
> >> 02:55:08.464074 IP (tos 0x20, ttl 48, id 33303, offset 0, flags
> >> [DF], length:
> >> 57) 198.82.160.221.8582 > 69.17.112.250.53: [udp sum ok] 0 A?
> >> tpmcafe.com. (29)
> >> 02:55:08.465514 IP (tos 0x0, ttl 63, id 0, offset 0, flags [DF],
> >> length: 529)
> >> 69.17.112.250.53 > 198.82.160.221.8582: [udp sum ok] 0- 0/13/14
> >> (501)
> >> 02:55:12.148692 IP (tos 0x20, ttl 48, id 33639, offset 0, flags
> >> [DF], length:
> >> 72) 198.82.160.221.8582 > 69.17.112.250.53: [udp sum ok] 0 A?
> >> connect.hillaryclinton.com. (44)
> >> 02:55:12.150062 IP (tos 0x0, ttl 63, id 0, offset 0, flags [DF],
> >> length: 528)
> >> 69.17.112.250.53 > 198.82.160.221.8582: [udp sum ok] 0- 0/13/13
> >> (500)
> >> 02:55:12.207552 IP (tos 0x20, ttl 48, id 33726, offset 0, flags
> >> [DF], length:
> >> 57) 198.82.160.221.8582 > 69.17.112.250.53: [udp sum ok] 0 A?
> >> www.ajc.com. (29)
> >> 02:55:12.208921 IP (tos 0x0, ttl 63, id 0, offset 0, flags [DF],
> >> length: 529)
> >> 69.17.112.250.53 > 198.82.160.221.8582: [udp sum ok] 0- 0/13/14
> >> (501)
> >> homer.ka9q.net. A 69.17.112.250 (222)
> >> 02:55:13.945772 IP (tos 0x20, ttl 48, id 33852, offset 0, flags
> >> [DF], length:
> >> 57) 198.82.160.221.8582 > 69.17.112.250.53: [udp sum ok] 0 A?
> >> youtube.com. (29)
> >> 02:55:13.947151 IP (tos 0x0, ttl 63, id 0, offset 0, flags [DF],
> >> length: 529)
> >> 69.17.112.250.53 > 198.82.160.221.8582: [udp sum ok] 0- 0/13/14
> >> (501)
> >> 02:55:19.121235 IP (tos 0x20, ttl 48, id 34282, offset 0, flags
> >> [DF], length:
> >> 62) 198.82.160.221.8582 > 69.17.112.250.53: [udp sum ok] 0 A?
> >> drudgereport.com.
> >> (34)
> >> 02:55:19.122727 IP (tos 0x0, ttl 63, id 0, offset 0, flags [DF],
> >> length: 534)
> >> 69.17.112.250.53 > 198.82.160.221.8582: [udp sum ok] 0- 0/13/14
> >> (506)
> >> 02:55:22.793109 IP (tos 0x20, ttl 48, id 34501, offset 0, flags
> >> [DF], length:
> >> 71) 198.82.160.221.8582 > 69.17.112.250.53: [udp sum ok] 0 A?
> >> www.desmoinesregister.com. (43)
> >> 02:55:22.794525 IP (tos 0x0, ttl 63, id 0, offset 0, flags [DF],
> >> length: 527)
> >> 69.17.112.250.53 > 198.82.160.221.8582: [udp sum ok] 0- 0/13/13
> >> (499)
> >> 02:55:24.093259 IP (tos 0x20, ttl 48, id 34638, offset 0, flags
> >> [DF], length:
> >> 66) 198.82.160.221.8582 > 69.17.112.250.53: [udp sum ok] 0 A?
> >> www.mysanantonio.com. (38)
> >> 02:55:24.094675 IP (tos 0x0, ttl 63, id 0, offset 0, flags [DF],
> >> length: 538)
> >> 69.17.112.250.53 > 198.82.160.221.8582: [udp sum ok] 0- 0/13/14
> >> (510)
> >> 02:55:24.320412 IP (tos 0x20, ttl 48, id 34677, offset 0, flags
> >> [DF], length:
> >> 57) 198.82.160.221.8582 > 69.17.112.250.53: [udp sum ok] 0 A?
> >> www.cnn.com. (29)
> >> 02:55:24.321856 IP (tos 0x0, ttl 63, id 0, offset 0, flags [DF],
> >> length: 529)
> >> 69.17.112.250.53 > 198.82.160.221.8582: [udp sum ok] 0- 0/13/14
> >> (501)
> >> 02:55:26.569416 IP (tos 0x20, ttl 48, id 34874, offset 0, flags
> >> [DF], length:
> >> 59) 198.82.160.221.8582 > 69.17.112.250.53: [udp sum ok] 0 A?
> >> www.omaha.com. (31)

> >> 02:55:26.570838 IP (tos 0x0, ttl 63, id 0, offset 0, flags [DF],
> >> length: 531)
> >> 69.17.112.250.53 > 198.82.160.221.8582: [udp sum ok] 0- 0/13/14
> >> (503)
> >> 02:55:27.288581 IP (tos 0x20, ttl 48, id 34954, offset 0, flags
> >> [DF], length:
> >> 68) 198.82.160.221.8582 > 69.17.112.250.53: [udp sum ok] 0 A?
> >> www.delawareonline.com. (40)
> >> 02:55:27.289962 IP (tos 0x0, ttl 63, id 0, offset 0, flags [DF],
> >> length: 540)
> >> 69.17.112.250.53 > 198.82.160.221.8582: [udp sum ok] 0- 0/13/14
> >> (512)
> >> 02:55:27.780863 IP (tos 0x20, ttl 48, id 35001, offset 0, flags
> >> [DF], length:
> >> 66) 198.82.160.221.8582 > 69.17.112.250.53: [udp sum ok] 0 A?
> >> www.sun-sentinel.com. (38)
> >> 02:55:27.782342 IP (tos 0x0, ttl 63, id 0, offset 0, flags [DF],
> >> length: 538)
> >> 69.17.112.250.53 > 198.82.160.221.8582: [udp sum ok] 0- 0/13/14
> >> (510)
> >> 02:55:31.298204 IP (tos 0x20, ttl 48, id 35326, offset 0, flags
> >> [DF], length:
> >> 61) 198.82.160.221.8582 > 69.17.112.250.53: [udp sum ok] 0 A?
> >> www.expedia.com. (33)
> >> 02:55:31.299562 IP (tos 0x0, ttl 63, id 0, offset 0, flags [DF],
> >> length: 533)
> >> 69.17.112.250.53 > 198.82.160.221.8582: [udp sum ok] 0- 0/13/14
> >> (505)
> >>
> >> ----- End forwarded message -----
> >>
> >>
> >>
> >> Please contact zorba at vt.edu and PlanetLab Support immediately.
> >> Explain the nature of your experiment, as well as the purpose of
> >> the traffic.
> >>
> >> PlanetLab Support <support at planet-lab.org>
> >>
> >
> >
> >
> > Bill Marmagas
> > Senior Systems Engineer
> > Systems Engineering & Administration
> > Virginia Tech
> >
> >
>
>
> Bill Marmagas
> Senior Systems Engineer
> Systems Engineering & Administration
> Virginia Tech
>
>
>
> Since I have not had a response yet, I am rebooting this node into debug state so that it is off-line to researchers but available to Planet-Lab sysadmi
>
>
>
> On Feb 14, 2008, at 10:31 AM, Bill Marmagas wrote:
>
>
> Begin forwarded message:
>
> From: PlanetLab Support <support at planet-lab.org>
> Date: February 14, 2008 10:27:44 AM EST
> To: princeton_traffic at slices.planet-lab.org
> Cc: support at planet-lab.org, zorba at vt.edu
> Subject: PlanetLab Traffic Report Feedback - princeton_traffic
> Reply-To: PlanetLab Support <support at planet-lab.org>
>
>
>
> PlanetLab Traffic Report Feedback - princeton_traffic
>
> PlanetLab has received feedback from zorba at vt.edu regarding
> the following traffic transmitted by your slice:
>
> Start Time: Feb 13 23:09:14
> End Time: Feb 13 23:59:50
> Slice: princeton_traffic
> Protocol: UDP
> Source IP: bob.cc.vt.edu
> Source Port: n/a
> Destination IP: 69.17.112.250
> Destination Port: domain (53)
> KPackets: 0.91
> KBytes: 55.74
>
> Comments:
> Virginia Tech received the following abuse report that seems to be related to your research slice:
>
> ----- Forwarded message from Phil Karn -----
>
> Date: Wed, 13 Feb 2008 19:17:53 -0800
> From: Phil Karn
> To: benchoff at vt.edu, abuse at vt.edu
> Subject: [ABUSE] Network abuse report
>
> Hi. You are listed as the technical contact in 'whois' for vt.edu.
> I couldn't
> find a specific abuse reporting address listed so I am sending to
> you as well as
> "abuse at vt.edu". If you are not the right person to handle computer
> security
> incidents, please forward this to the correct person.
>

> I am seeing a steady stream of requests to my DNS server from a
> computer at VT.
> The IP address is 198.82.160.221, which resolves back to
> bob.cc.vt.edu.
>
> The queries are for a long list of well known domain names, e.g.,
> www.yahoo.com
> or www.cnn.com. There are far too many kinds of attacks on the
> Internet for me
> to be familiar with the details of every one, but I suspect this
> is a "cache
> poisoning" attempt. I.e., if he can find a domain entry already in
> my cache, he
> can try to replace it with an unsolicited response so that when I
> visit that
> site again, I can be steered to a different IP address.
>
> I believe my version of the BIND nameserver is resistant to this
> particular
> attack; it answers every remote request with an error whether or
> not the
> requested domain is already in my cache, so his scanning is
> pointless. But I
> would like to report it anyway as whoever is doing this is
> probably attacking
> many other systems. You may also wish to examine bob.cc.vt.edu in
> case it has
> been compromised by a remote party and is being used to launch
> these attacks.
>
> Thanks,
>
> Phil Karn
>
> P.S. I have appended a packet trace of a small sample of the
> queries. My
> apologies for the way lines are wrapped.
>
> 2:54:55.888977 IP (tos 0x20, ttl 48, id 32520, offset 0, flags
> [DF], length:
> 59) 198.82.160.221.8582 > 69.17.112.250.53: [udp sum ok] 0 A?
> www.yahoo.com. (31)
> 02:54:55.890467 IP (tos 0x0, ttl 63, id 0, offset 0, flags [DF],
> length: 531)
> 69.17.112.250.53 > 198.82.160.221.8582: [udp sum ok] 0- 0/13/14
> (503)
> 02:55:08.464074 IP (tos 0x20, ttl 48, id 33303, offset 0, flags
> [DF], length:
> 57) 198.82.160.221.8582 > 69.17.112.250.53: [udp sum ok] 0 A?
> tpmcafe.com. (29)
> 02:55:08.465514 IP (tos 0x0, ttl 63, id 0, offset 0, flags [DF],
> length: 529)
> 69.17.112.250.53 > 198.82.160.221.8582: [udp sum ok] 0- 0/13/14
> (501)
> 02:55:12.148692 IP (tos 0x20, ttl 48, id 33639, offset 0, flags
> [DF], length:
> 72) 198.82.160.221.8582 > 69.17.112.250.53: [udp sum ok] 0 A?
> connect.hillaryclinton.com. (44)
> 02:55:12.150062 IP (tos 0x0, ttl 63, id 0, offset 0, flags [DF],
> length: 528)
> 69.17.112.250.53 > 198.82.160.221.8582: [udp sum ok] 0- 0/13/13
> (500)
> 02:55:12.207552 IP (tos 0x20, ttl 48, id 33726, offset 0, flags
> [DF], length:
> 57) 198.82.160.221.8582 > 69.17.112.250.53: [udp sum ok] 0 A?
> www.ajc.com. (29)
> 02:55:12.208921 IP (tos 0x0, ttl 63, id 0, offset 0, flags [DF],
> length: 529)
> 69.17.112.250.53 > 198.82.160.221.8582: [udp sum ok] 0- 0/13/14
> (501)
> homer.ka9q.net. A 69.17.112.250 (222)
> 02:55:13.945772 IP (tos 0x20, ttl 48, id 33852, offset 0, flags
> [DF], length:
> 57) 198.82.160.221.8582 > 69.17.112.250.53: [udp sum ok] 0 A?
> youtube.com. (29)
> 02:55:13.947151 IP (tos 0x0, ttl 63, id 0, offset 0, flags [DF],
> length: 529)
> 69.17.112.250.53 > 198.82.160.221.8582: [udp sum ok] 0- 0/13/14
> (501)
> 02:55:19.121235 IP (tos 0x20, ttl 48, id 34282, offset 0, flags
> [DF], length:
> 62) 198.82.160.221.8582 > 69.17.112.250.53: [udp sum ok] 0 A?
> drudgereport.com.
> (34)
> 02:55:19.122727 IP (tos 0x0, ttl 63, id 0, offset 0, flags [DF],
> length: 534)
> 69.17.112.250.53 > 198.82.160.221.8582: [udp sum ok] 0- 0/13/14
> (506)
> 02:55:22.793109 IP (tos 0x20, ttl 48, id 34501, offset 0, flags
> [DF], length:
> 71) 198.82.160.221.8582 > 69.17.112.250.53: [udp sum ok] 0 A?
> www.desmoinesregister.com. (43)
> 02:55:22.794525 IP (tos 0x0, ttl 63, id 0, offset 0, flags [DF],
> length: 527)
> 69.17.112.250.53 > 198.82.160.221.8582: [udp sum ok] 0- 0/13/13
> (499)
> 02:55:24.093259 IP (tos 0x20, ttl 48, id 34638, offset 0, flags
> [DF], length:
> 66) 198.82.160.221.8582 > 69.17.112.250.53: [udp sum ok] 0 A?
> www.mysanantonio.com. (38)
> 02:55:24.094675 IP (tos 0x0, ttl 63, id 0, offset 0, flags [DF],
> length: 538)
> 69.17.112.250.53 > 198.82.160.221.8582: [udp sum ok] 0- 0/13/14
> (510)
> 02:55:24.320412 IP (tos 0x20, ttl 48, id 34677, offset 0, flags
> [DF], length:
> 57) 198.82.160.221.8582 > 69.17.112.250.53: [udp sum ok] 0 A?
> www.cnn.com. (29)
> 02:55:24.321856 IP (tos 0x0, ttl 63, id 0, offset 0, flags [DF],
> length: 529)

> 69.17.112.250.53 > 198.82.160.221.8582: [udp sum ok] 0- 0/13/14
> (501)
> 02:55:26.569416 IP (tos 0x20, ttl 48, id 34874, offset 0, flags
> [DF], length:
> 59) 198.82.160.221.8582 > 69.17.112.250.53: [udp sum ok] 0 A?
> www.omaha.com. (31)
> 02:55:26.570838 IP (tos 0x0, ttl 63, id 0, offset 0, flags [DF],
> length: 531)
> 69.17.112.250.53 > 198.82.160.221.8582: [udp sum ok] 0- 0/13/14
> (503)
> 02:55:27.288581 IP (tos 0x20, ttl 48, id 34954, offset 0, flags
> [DF], length:
> 68) 198.82.160.221.8582 > 69.17.112.250.53: [udp sum ok] 0 A?
> www.delawareonline.com. (40)
> 02:55:27.289962 IP (tos 0x0, ttl 63, id 0, offset 0, flags [DF],
> length: 540)
> 69.17.112.250.53 > 198.82.160.221.8582: [udp sum ok] 0- 0/13/14
> (512)
> 02:55:27.780863 IP (tos 0x20, ttl 48, id 35001, offset 0, flags
> [DF], length:
> 66) 198.82.160.221.8582 > 69.17.112.250.53: [udp sum ok] 0 A?
> www.sun-sentinel.com. (38)
> 02:55:27.782342 IP (tos 0x0, ttl 63, id 0, offset 0, flags [DF],
> length: 538)
> 69.17.112.250.53 > 198.82.160.221.8582: [udp sum ok] 0- 0/13/14
> (510)
> 02:55:31.298204 IP (tos 0x20, ttl 48, id 35326, offset 0, flags
> [DF], length:
> 61) 198.82.160.221.8582 > 69.17.112.250.53: [udp sum ok] 0 A?
> www.expedia.com. (33)
> 02:55:31.299562 IP (tos 0x0, ttl 63, id 0, offset 0, flags [DF],
> length: 533)
> 69.17.112.250.53 > 198.82.160.221.8582: [udp sum ok] 0- 0/13/14
> (505)
>
> ----- End forwarded message -----
>
>
>
> Please contact zorba at vt.edu and PlanetLab Support immediately.
> Explain the nature of your experiment, as well as the purpose of the traffic.
>
> PlanetLab Support <support at planet-lab.org>
>
>
>
>
>
> Bill Marmagas
> Senior Systems Engineer
> Systems Engineering & Administration
> Virginia Tech
>
>
>
>
>
> Bill Marmagas
> Senior Systems Engineer
> Systems Engineering & Administration
> Virginia Tech
>
>
> _____
> PlanetLab Support Mail Reflector
> support at planet-lab.org
> https://lists.planet-lab.org/mailman/listinfo/support-community
>
>

- Previous message: [PL #24059] planetlab1.tmit.bme.hu - abuse
- Next message: [PL #24059] planetlab1.tmit.bme.hu - abuse
- **Messages sorted by:** [date] [thread] [subject] [author]

More information about the support-community mailing list