

RE: unidentified DOS "bad traffic"

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/incidents/2003-03/0142.html>

From: David Gillett (gillettdavid@fhda.edu)

Date: 03/14/03

From: "David Gillett" <gillettdavid@fhda.edu>

To: <incidents@securityfocus.com>

Date: Thu, 13 Mar 2003 15:26:41 -0800

We've seen a couple of incidents similar to this lately (although we haven't been able to capture as much detail).

My working hypothesis is that this is an attempt at a DDoS aimed at "irc-m.icq.aol.com", but that due to a bug or design error, it takes down the source network instead.

We did see flooding that brought down internal traffic without loading the routers. The routers did, however, log a spike in inbound traffic volume right around that time, suggesting an external trigger mechanism....

David Gillett

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

> From: DY [<mailto:dybulk@tri8.net>]

> Sent: March 13, 2003 13:54

> To: incidents@securityfocus.com

> Subject: unidentified DOS "bad traffic"

>

>

> Hi all,

>

> I'm quite surprised at the lack of material I'm turning up in

> researching

> this issue, so I'm resorting to this post. Please feel free

> to point me

> somewhere.

>

> Twice in the past week I have experienced a severe DOS condition on my

> network. A particular host has been completely flooding the

> network with

> some sort of traffic that chokes the whole thing. Now, on the first

> incident I was unable to obtain packet trace data (I'll spare

> the details)

> and was forced to reconnect the particular segment's port.

RE: unidentified DOS "bad traffic"

SecurityFocus Incidents: RE: unidentified DOS "bad traffic"

> scanned his
> machine with the latest AV updates, with no viri found.
> 3) IP address 64.12.165.57, the destination for this complete flood of
> "bad traffic," resolves (reverse) to irc-m.icq.aol.com.
> 4) There was so much of this traffic that it shut my network down. My
> main router (Cisco) reported no appreciable CPU consumption during the
> attack. It just appears that the sheer volume of the [bad]
> packets choked
> everybody out.
>
>
> So, I know of no exploit, no virus, no known malicious
> destination (which
> might lead me to an exploit)...and yet I had no throughput
> (except for the
> "bad traffic").
>
> Can anybody give me a clue, or at least point me somewhere (probably
> obvious) that I seem to be missing? I might post to the
> Snort-users list
> as well, I guess, in case anybody there has ideas.
>
> Many TIA,
> --
> DY
>
> -----
> -----
>
> <Pre>Lose another weekend managing your IDS?
> Take back your personal time.
> 15-day free trial of StillSecure Border Guard.</Pre>
>
<http://www.securityfocus.com/stillsecure>

<Pre>Lose another weekend managing your IDS?
Take back your personal time.
15-day free trial of StillSecure Border Guard.</Pre>
 <http://www.securityfocus.com/stillsecure>