

Re: unidentified DOS 'bad traffic'

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/incidents/2003-03/0141.html>

From: Kerry Thompson (kerry@crypt.gen.nz)

Date: 03/14/03

Date: Fri, 14 Mar 2003 12:10:12 +1300 (NZDT)
From: "Kerry Thompson" <kerry@crypt.gen.nz>
To: <incidents@securityfocus.com>

GTBot (a DDOS agent) uses IP protocol 255 to communicate, sometimes large and/or small packets, and sometimes fragmented. Its quite capable of flooding most gateways, and connects to an IRC channel as you describe. You'd best read Dave Dittrich's paper at :

<http://staff.washington.edu/dittrich/talks/core02/xdcc-analysis.txt>

and look for the symptoms that he describes on the Win2k box.

Kerry

DY said:

> *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. We*
> *got by for a few days, and then wham, it happened again. This time I*
> *isolated the segment with a Snort sensor and captured a large amount of*
> *data (actually, I only sniffed for a few seconds before I'd already*
> *swallowed about 10 MB of data, all of which was identical, so I*
> *stopped). My Snort output on this trace was filled with nothing but*
> *bizillions of these entries (payload did vary a little):*
>
>
> *03/13-07:53:50.650383 10.1.2.3 -> 64.12.165.57*
> *PROTO255 TTL:128 TOS:0x0 ID:50456 IpLen:20 DgmLen:80*
> *45 10 00 3C B5 F5 40 00 40 06 E8 85 CD A2 E9 48 E..<..@.@.....H*
> *40 0C A5 39 D3 A6 1A 0B BC C0 DE 3C 00 00 00 00 @..9.....<....*
> *A0 02 7D 78 D3 8E 00 00 02 04 05 B4 04 02 08 0A ..}x.....*

SecurityFocus Incidents: Re: unidentified DOS 'bad traffic'

> 00 CD 7F 52 52 00 00 00 01 03 03 00 ...RR.....

>

>

=+++++

>

>

>

> *The source IP is from a private network that I run, which uses basic
> NAT, so I can certainly route and identify the host, as this capture is
> from the private side of the NAT router. Now, here's the Snort alert
> entry (again, just thousands of this same entry):*

>

>

> *[**] [1:1627:1] BAD TRAFFIC Unassigned/Reserved IP protocol [**]*

> *[Classification: Detection of a non-standard protocol or event]*

> *[Priority: 2]*

> *03/13-07:53:11.032136 10.1.2.3 -> 64.12.165.57*

> *PROTO255 TTL:128 TOS:0x0 ID:23977 IpLen:20 DgmLen:80*

>

>

> *Now, I've read up on the Snort signature that generates this alert (SID
> 1627). It says that it's bad traffic (of course) using an unassigned
> protocol, which of course the alert states. However, I'm not finding
> anything (Google, Usenet, etc.) that leads me toward the proper analysis
> of what this machine was doing. All I know is:*

>

> *1) The machine runs Win2K pro.*

> *2) The user has no idea what's going on, of course, and has 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.*

<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>