




[Home](#) | [Resources](#) | [News](#) | [Travel](#) | [Shopping](#) | [Finance](#) | [Careers](#) | [Education](#) | [Military Jobs](#) | [Community](#)

» You are not logged in. [Login](#) or [register](#)

[MyPop™](#) | [register](#) | [faq](#) | [search](#)

DISCUSSION BOARDS



[New Topic](#)
[Post a Poll](#)
[* PopI](#)

 [Email this page to someone!](#)

[Military.com Forums](#) » [Hot Topics & Current Events](#) » [Point-Counterpoint](#) » MASSIVE DDOS ATTACKS ALL OVER U.S.

Author

AmericanIntel

Basic Training

Registered: Friday, 03
January 2003
Posts: 13

Topic: MASSIVE DDOS ATTACKS ALL OVER U.S.

MASSIVE DDOS ATTACKS ALL OVER U.S.

We are monitoring massive Distributed Denial of Service attacks all over the U.S. starting at around 11:30 PM CST. As many as 5 of the 13 root nameserver have b up to 10 with massive packet loss (xx%):

Internet Status to Root Name Servers
Date: Fri Jan 24 21:37:00 PST 2003

Place Address Packet Loss Time: Min/Avg/Max

Root b.root-servers.net 53% 25/40/48
Root c.root-servers.net 0% 82/82/82
Root e.root-servers.net 20% 16/29/33
Root f.root-servers.net 26% 17/27/32
Root h.root-servers.net 20% 91/101/108
Root i.root-servers.net 26% 190/199/205
Root j.root-servers.net 26% 81/91/96
Root k.root-servers.net 64% 172/188/201
Root l.root-servers.net 0% 5/5/6
Root m.root-servers.net 33% 160/171/205
GTLD b.gtld-servers.net 26% 52/63/67
GTLD c.gtld-servers.net 31% 85/93/95
GTLD d.gtld-servers.net 13% 88/100/103
GTLD f.gtld-servers.net 22% 38/50/57
GTLD i.gtld-servers.net 0% 198/200/203
GTLD k.gtld-servers.net 24% 90/100/105
GTLD l.gtld-servers.net 33% 128/138/171

All backbone providers are suffering major packet loss (XX%):

Place Address Packet Loss Time: Min/Avg/Max

AboveNet ns.above.net 28% 53/64/66
AGIS ns1.agis.net 26% 62/74/78
AlohaNet nuhou.aloha.net 35% 84/94/98
ANS ns.ans.net 26% 83/97/100
BBN-NearNet nic.near.net 28% 91/114/572
BBN-BARRnet ns1.barrnet.net 26% 16/26/32
Best ns.best.com 35% 79/89/95
Concentric nameserver.concentric.net 35% 18/31/56
CW ns.cw.net 28% 88/98/105

DIGEX ns.digex.net 31% 78/86/91
 ENTER.NET dns.enter.net 28% 91/104/108
 Epoch Internet ns1.hlc.net 33% 37/48/52
 Flash net ns1.flash.net 17% 80/92/94
 GetNet ns1.getnet.com 20% 40/52/56
 GlobalCrossing name.roc.gblx.net 24% 85/97/104
 GoodNet ns1.good.net 31% 83/92/97
 GridNet grid.net 20% 80/92/101
 IDT Net ns.idt.net 20% 91/104/121
 Internex nic1.internex.net 26% 18/31/35
 MCI ns.mci.net 22% 91/103/107
 MindSpring itchy.mindspring.net 15% 75/88/106
 NAP.NET ns2.nap.net 20% 73/85/94
 PacBell ns1.pbi.net 0% 89/89/90
 Primenet dns1.primenet.net 20% 31/41/45
 PSI ns.psi.net 0% 82/84/160
 RAINet ns.rain.net 31% 40/49/53
 SAVVIS ns1.savvis.net 31% 88/99/102
 SprintLink ns1.sprintlink.net 11% 15/27/35
 UUNet,AlterNet auth00.ns.uu.net 26% 89/98/103
 Verio-West ns0.verio.net 22% 31/42/47
 Verio-East ns1.verio.net 22% 86/96/101
 VISInet ceylon.visinet.ca 20% 102/116/188
 MoonGlobal-ClubNET ns.clubnet.net 0% 0/1/2
 MoonGlobal-Netway dns.nwc.net 4% 6/6/7
 MoonGlobal-Netxactics verdi.netxactics.com 4% 6/6/7
 InterWorld ns.interworld.net 0% 4/4/5

It's massive, no word on source yet. We are watching it closely.

Brad G
 American Intelligence
www.americanintelligence.us

📅 posted **Fri, 24 January 03** 22:5

Brian_Cz
 Basic Training

Registered: Sunday, 19
 January 2003
 Posts: 7

Major Attack!

Yes i noticed the start of this about 2 hours ago. it seems to be affecting udp port kind of worm exploiting mysql server. It may or may not be a DoS attack. Its mes everything up, good think its the middle of the night.

📅 posted **Sat, 25 January 03** 00:3

Asus1
 Basic Training

Registered: Saturday,
 25 January 2003
 Posts: 8

Oh and I bet you think that US is the centre of world did u consider other country:
 here
 some ppl or countries with there 1 track mind get out of the dirt 😊

📅 posted **Sat, 25 January 03** 01:0

WillFarnaby
 Basic Training

Registered: Saturday,
 25 January 2003
 Posts: 2

Learn to read

"We are monitoring massive Distributed Denial of Service attacks all over the U.S.

You see.. that says "all over the U.S." where it is currently nighttime.

That being said, this is really f**king with me as I am trying to get some webdev my sites are all down, or at least not accessible to me.

📅 posted **Sat, 25 January 03** 01:1

TheBladeRoden
Basic Training

It's Tom Ridge's security measures taking effect

Registered: Saturday,
25 January 2003
Posts: 1

BTW I love his haircut

📅 posted **Sat, 25 January 03** 02:0

virtualinsanity
Basic Training

hmmm....other dudes say that there isnt any attack..u may have any other source news ?

Registered: Saturday,
25 January 2003
Posts: 3

l8er

📅 posted **Sat, 25 January 03** 02:0

WillFarnaby
Basic Training

I don't know if there's an attack or not, but something is definitely up.

Registered: Saturday,
25 January 2003
Posts: 2

Like I said, I can't get to any of my sites and <http://www.internethealthreport.com> showing that UUnet/Worldcom is screwed. Earlier tonight all of Internap was in the

It looks like now most of the problems are centered in Dallas.

📅 posted **Sat, 25 January 03** 02:0

Asus1
Basic Training

Learn to read "We are monitoring massive Distributed Denial of Service attacks all U.S. tonight..."

Registered: Saturday,
25 January 2003
Posts: 8

You see.. that says "all over the U.S." where it is currently nighttime.

That being said, this is really f**king with me as I am trying to get some webdev my sites are all down, or at least not accessible to me.

=====posted by the willy

erm 1 did i say i was talking to you i can read nicely but your point is really beside dont or is it that 1 track mind agin?

📅 posted **Sat, 25 January 03** 02:1

Asus1
Basic Training

BTW I originaly said that to Brian_Cz
:/ get ya head out of the dirt willy 🤪

Registered: Saturday,
25 January 2003
Posts: 8

📅 posted **Sat, 25 January 03** 02:2

Lagoudakos
Basic Training

🤪 hehe that's funny

Registered: Saturday,
25 January 2003
Posts: 1

Guys i think this mysql problem has been given a patch since 6 months have a look at cert

<http://www.kb.cert.org/vuls/id/370308>

i cannot understand you can find so many bugs for MS
i think they try on purpose to make the bugs
it cannot be coincidence to have so many
:P

📅 posted **Sat, 25 January 03** 02:3

Richto

Basic Training

Thats not mysql - thats MS SQL. Cant you read?

Registered: Saturday,
25 January 2003
Posts: 3

📅 posted **Sat, 25 January 03** 03:2

RavMT

Basic Training

Holy Crap!

Under my careful Confirmations with my leet MTer buddies

Registered: Saturday,
25 January 2003
Posts: 1

I have calculated that there is a skill check in osmethne!

This is a Crisis people! 🤖 🤖

📅 posted **Sat, 25 January 03** 03:3

djvidman

Basic Training

🔍 Check this site..

Registered: Saturday,
25 January 2003
Posts: 1

Packet Loss & IP Reachability charts updated every hour:

<http://average.matrix.net>

[This message was edited by djvidman on Saturday, 25 January 2003 at 04:00.]

📅 posted **Sat, 25 January 03** 03:5

StealthMode

Basic Training

DDoS attacks....

Registered: Saturday,
25 January 2003
Posts: 1

As to the DDoS attacks (thats the acronym). They are old news. Starting what was September/October of last year, the www root servers (the ones that tell ur comp the http address www.website.com is assigned to) were attacked using a simple D service bug. The interesting thing here was the huge amount of traffic that was flc root servers. It wasnt just one or two or even a dozen machines. It was over a mi them. My thing? I say its a virus or trojan that at certain times (triggered by a dat even a simple packet sent out by the creator) will start transmitting the DDoS targ www root servers. This is old news. The guy who posted bout it starting back up is He/she must not have been aware of the Sept./Oct. incidents....I believe it is mor widespread now. That is why you are seeing it cover more of the root servers and original 5 it targeted.

-StealthMode
USN IRR

📅 posted **Sat, 25 January 03** 04:2

corto

Basic Training

the MS security bulletin

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bu>

Registered: Friday, 27
December 2002
Posts: 21

[039.asp](#)

admin who operate MS-sql can fix theirs computers if they dont have already done

📅 posted **Sat, 25 January 03** 04:3

D3T
Basic Training

Isnt DRDoS more aproprate

Registered: Saturday,
25 January 2003
Posts: 2

Considering there is many sources of this "attack", and considering there is likely 200 PCs involved in kicking it off, having found and developed programs to exploit weakness, the Term DRDoS (Distributed Reflected Denial of Service) seems more Where traffic is bounced off affected servers? right?

📅 posted **Sat, 25 January 03** 05:2

HHans
Basic Training

🤖 some was ask me to give root at me server just read ...

Registered: Saturday,
25 January 2003
Posts: 3

some ask me for root for 30 last night mins crazy i think ... Poll Question:
some was ask last night to get root for 30 mins he had no way to go but strange a
last night was an idiot from some servers
on mine chat server and was ask for root for 30 mins
juts i think this figures like to hack things
we have kline him after pushing to get root access on me server ...
strange enough than i now read this all
wen some like to post at our caht server please tel us
maybe you can get the persons may that do this
we have never before see any such users that was ask
about starnge things
ps wen some will see things
log at icq.zapto.org port 6667 on a mirc chat client wen you not have that downlo:
site
<http://members.chello.nl/~h.meesters/index>
maye we can get the persons
.
the nickname from the person was One_lamer*@w3 &
Apokalipse << host Pasarika@gepedo.astral.ro << i think that host is fake from tl
>>>
i think its a very dangerous person hes kiline..

afz Hans Netherlands

📅 posted **Sat, 25 January 03** 05:5

D3T
Basic Training

Op/root begging is not uncommon, however i dont think it's anything too serious.
Klined him it should be sorted -- he cant connect and can certainly not get root ac
because his address is banned, and you have to ident with the server to get your i
Might be best to get a decent firewall if you think he might try something on you.
free edition is -great- wheras blackice defender is -awful-).

Registered: Saturday,
25 January 2003
Posts: 2

📅 posted **Sat, 25 January 03** 06:3

dhd
Basic Training

worm analysis

Registered: Saturday,
25 January 2003

this is simply a worm, an analysis of which can be found here:

Posts: 1

http://www.digitaloffense.net/worms/mssql_udp_worm
 posted **Sat, 25 January 03** 06:4
AmericanIntel

Basic Training

Registered: Friday, 03
January 2003

Posts: 13

Hey Asus... give it a rest! When I first posted this 5 of the 13 root name servers that went down were all in the U.S.. Most of the backbone providers that were down were all in the U.S.. We hadn't captured a packet yet and didn't know what the cause was at the time. We weren't able to connect to military.com to update.

This affected everyone around the world but the U.S. was hardest hit as far as we

 posted **Sat, 25 January 03** 07:1
mdella

Basic Training

Registered: Saturday,
25 January 2003

Posts: 1

DDoS worm via MS SQL (pre-SP2) on port 1434/UDP

Just in case anyone wanted a more complete story of what is happening...

There is a worm spreading RAPIDLY throughout the world (regardless of border, etc). It is targeting port 1434/UDP specifically targeting a security vulnerability

<http://www.nextgenss.com/advisories/mssql-udp.txt>

that has apparently been patched with SP2. Still unclear if this is the specific issue. The worm is hitting.

The worm then uses the maximum bandwidth to "spray" itself to any IP address in its target mode. This volume and non-directional spray is causing overloads in network switches as backbone routers.

Starting around midnight (PST) backbone operators throughout the world began finding 1434/UDP on both inbound as well as outbound interfaces.

The US only appears to be hardest hit because with the greater bandwidth between the US and the rest of the world it has a more spectacular effect of the spraying. It is no less a problem anywhere in the world however.

The main reason for the root servers to go down have nothing to do with the servers themselves. The dang equipment between you and them. Most backbone routers were running at 100% CPU since 9:30pm PST until around 1-2am PST where people started getting a gridlock of traffic...

Marcos

 posted **Sat, 25 January 03** 07:3
Asus1

Basic Training

Registered: Saturday,
25 January 2003

Posts: 8

well ok then ill give it a rest i just wont share the valuable information of this attack with you one then im sure i have all the inside info and details how it actually works perfectly

 posted **Sat, 25 January 03** 07:3
Asus1

Basic Training

Registered: Saturday,
25 January 2003

Posts: 8

look at the typos :P basically ill just not share what i know and have..

 posted **Sat, 25 January 03** 07:3
Asus1

Basic Training

/me coughs and points at part of the code

Registered: Saturday,
25 January 2003
Posts: 8

```
char exploit_code[]=
"\x55\x8B\xEC\x68\x18\x10\xAE\x42\x68\x1C"
"\x10\xAE\x42\xEB\x03\x5B\xEB\x05\xE8\xF8"
.....to be continued :P
```

 posted **Sat, 25 January 03** 07:3

RalfT
Basic Training

SQL server

Registered: Saturday,
25 January 2003
Posts: 1

It is not true that SP2 for MS sqlserver is patching this problem, you have to have

 posted **Sat, 25 January 03** 07:3

Brian_Cz
Basic Training

Asus??

Registered: Sunday, 19
January 2003
Posts: 7

Asus whats your problem, his post said monitoring all over the U.S. it was the mid night for me, and yes i was on my way to bed so i made a quick post. I dont see v it so personal, it was a little mistake. It did hit the eastern united states first on th backbone, as of when i posted, so it was not affecting everyone at that time. You seriously loosen up!

 posted **Sat, 25 January 03** 07:5

Asus1
Basic Training

RalfT correct and brian ur a dim minded dip ****..

Registered: Saturday,
25 January 2003
Posts: 8

 posted **Sat, 25 January 03** 08:0

Asus1
Basic Training

I can see amny reasons how many years of history shall we talk about?? brian?

Registered: Saturday,
25 January 2003
Posts: 8

 posted **Sat, 25 January 03** 08:1

nostgard
Basic Training

Asus1

Registered: Saturday,
25 January 2003
Posts: 1

I don't see why you're getting so worked up about someone who lives in the US b about the fact that its night time for him... should every person in the US take the world into account when making a generic statement about time? I mean, come o

 posted **Sat, 25 January 03** 08:2

GuildPortal
Basic Training

quote:

Registered: Saturday,
25 January 2003
Posts: 1

Originally posted by Lagoudakos:
i cannot understand you can find so many bugs for MS
i think they try on purpose to make the bugs
it cannot be coincidence to have so many
:P

Dude... The patch that fixes the vulnerability is over a year old. How is that Micros

Maybe if companies would conduct a little more thorough screening of applicants for positions, they'd get people who knew how to download and install service packs.

📅 posted **Sat, 25 January 03** 09:00

[New Topic](#) [Post a Poll](#) [Post Reply](#)



[Printable](#)



[Email a Friend](#)



[PopIt!](#)



[MyPop™](#)

Hop To:

[Contact Us](#) | [Military.com](#)

(c) 2003 Military Advantage, Inc.

Powered by INFOPOP ©2002

OpenTopic 3.0.4

[Military.com](#) | [Army](#) | [Navy](#) | [Air Force](#) | [Marines](#) | [Coast Guard](#) | [DoD](#)
[HistoryChannel.com](#) | [Affiliate Program](#) | [About Us](#) | [Help and Feedback](#)
[Advertising Info](#) | [Terms of Use](#) | [Privacy Policy](#)