

Forum:[Hack Forums](#)

Thread: [What makes some ddos viruses more powerful than others?](#)

SIM-4910472 - June 17, 2021, 11:43 pm

What makes some ddos viruses gbps higher than others, and how do they calculate their gbps?

shaino - June 18, 2021, 2:45 am

Some use a better ddosing technique than others do

SIM-4910472 - June 18, 2021, 2:27 pm

(Jun 18, 2021 02:45 AM)shaino Wrote: [\[CITE\]](#) Some use a better ddosing technique than others do
What are those other techniques?

shaino - June 18, 2021, 2:28 pm

(Jun 18, 2021 02:27 PM)SIM-4910472 Wrote: [\[CITE\]](#) What are those other techniques?
no idea, prob just sending stuff faster but im just guessing rn im not the guy to really ask

SIM-4910472 - June 18, 2021, 2:30 pm

(Jun 18, 2021 09:48 AM)Incog Wrote: [\[CITE\]](#) "Better ddosing technique"
You arent wrong but it's a very shit way of describing it.

People find bypasses, or people push their bots harder. If you send larger payloads for L4 you push more power, but at the same time stress the bot. same for L7 with threads.

You need to balance power over usages imo, no point in pushing it to the limit if the limit breaks it
What is L4 and L7?

SIM-4910472 - June 18, 2021, 2:43 pm

(Jun 18, 2021 02:41 PM)Incog Wrote: [\[CITE\]](#) Sorry I forgot not everyone uses those terms, they represent the Layers on the OSI model, so L4 (layer 4) is the transport level, focusing on tcp and udp attack based methods. L7 (layer 7) is the application level, so HTTP or HTTPS, focused on typically web based attacks for websites and so on.

I hope that cleared anything up.
Yes, thank

LogiTech - June 19, 2021, 3:02 am

I have no idea what's going on in that scene these days as far as protection and techniques used to bypass. There's basic denial of service attacks that rely on sheer volume. Others will target a specific protocol or services like Apache.

You should consider denial of service attacks a broad description as even maliciously cutting the power you have physical access to is considered a denial of service attack. That's a really dumb technicality, but I'm trying to reinforce my point that there's many ways to carry out a DoS attack.

Edit:

I just typed all that and realized I didn't answer your question the right way. It's not always about the volume of data you can dish out, but it is the easiest. Start with a google search on DNS amplification. It will give you an idea of why some attacks can be more efficient than others.

ownd - June 21, 2021, 7:26 am

I know this is sort of off topic but what would be a way currently to do so if there is something on the HF or someone that can perform it might want to get PM me for further educating me :)

SIM-4910472 - June 21, 2021, 7:17 pm

(Jun 20, 2021 06:18 PM)Dyne Wrote: [\[CITE\]](#) Very good explanation.

Also very worth noting and adding is the number of connections.

Botnet DDOS attacks are based on the number of connections and which socket can be exploited if it is a domain or website, port if its a direct IP or provisioned line if its a service.

Some more criminal DDOS stresser nets attack CO, which is based on DSL. DSLAM > BPX > Turnstone > Redback(L7).

These are typically more advanced provision line attacks which are meant to deter an entire service center (bank robbery, or larger criminal hit which relies on internet connection or VOIP to notify authorities, some choose to attack the service provider to buy more time).

DDOSing somebody on a video game or a website to obtain ransom, however, is a giant waste of time and a misdirected use of resources.

Why don't big companies like google or facebook get ddosed then?

Shadow_Cloud - June 21, 2021, 10:37 pm

(Jun 21, 2021 07:17 PM)SIM-4910472 Wrote: [\[CITE\]](#) Why don't big companies like google or facebook get ddosed then?

They do, all the time. You just get to a point where your mitigation is kicking in and you can scale horizontally on the fly.

SIM-4910472 - June 23, 2021, 3:21 am

(Jun 21, 2021 10:37 PM)Shadow_Cloud Wrote: [\[CITE\]](#) They do, all the time. You just get to a point where your mitigation is kicking in and you can scale horizontally on the fly. seems like a waste of time to try to ddos them.

(Jun 21, 2021 07:22 PM)Dyne Wrote: [\[CITE\]](#) for what? ransom?

you think they dont have backup SSL connections?

i don't know why they wouldn't

Shadow_Cloud - June 23, 2021, 3:24 am

(Jun 23, 2021 03:21 AM)SIM-4910472 Wrote: [\[CITE\]](#) seems like a waste of time to try to ddos them.

Yes but that's not quite the same as it not happening. The really trick attacks to get rid of are on layer7, they seem almost indistinguishable from your legit traffic. So as an example, slamming a website with registration requests from multiple sources using data that's hard to separate from actual users.

SIM-4910472 - June 23, 2021, 3:25 am

(Jun 23, 2021 03:24 AM)Shadow_Cloud Wrote: [\[CITE\]](#) Yes but that's not quite the same as it not happening. The really trick attacks to get rid of are on layer7, they seem almost indistinguishable from your legit traffic. So as an example, slamming a website with registration requests from

multiple sources using data that's hard to separate from actual users.
so it could be possible?

Shadow_Cloud - June 23, 2021, 3:27 am

(Jun 23, 2021 03:25 AM)SIM-4910472 Wrote: [\[CITE\]](#) so it could be possible?
Could what be possible? I'm not sure I understand your question?

SIM-4910472 - June 23, 2021, 3:29 am

(Jun 23, 2021 03:27 AM)Shadow_Cloud Wrote: [\[CITE\]](#) Could what be possible? I'm not sure I understand your question?
could it be possible to ddos google?

Shadow_Cloud - June 23, 2021, 3:31 am

(Jun 23, 2021 03:29 AM)SIM-4910472 Wrote: [\[CITE\]](#) could it be possible to ddos google?
Yes, but highly unlikely that you co-ordinate the resources required to make the attack effective, its far more likely that you could find a specific subsystem and affect their service delivery for that feature.

SIM-4910472 - June 23, 2021, 3:34 am

(Jun 23, 2021 03:31 AM)Shadow_Cloud Wrote: [\[CITE\]](#) Yes, but highly unlikely that you co-ordinate the resources required to make the attack effective, its far more likely that you could find a specific subsystem and affect their service delivery for that feature.
what if i had 5 million bots?

Shadow_Cloud - June 23, 2021, 3:39 am

(Jun 23, 2021 03:34 AM)SIM-4910472 Wrote: [\[CITE\]](#) what if i had 5 million bots?
You need to understand that there's a difference between the firepower you throw at it and how effective that firepower is. If you try to break a physical safe by throwing water balloons at it, I don't think it will matter how many million balloons you have. Purely having more might not be enough, especially not when a single mitigation technique can prevent any damage/influence from your attack vector.

These companies also don't run static configurations anymore. There's a dynamic landscape to deal with these things now.

bending - June 23, 2021, 3:44 am

(Jun 17, 2021 11:43 PM)SIM-4910472 Wrote: [\[CITE\]](#) What makes some ddos viruses gbps higher than others, and how do they calculate their gbps?
Simply its a combination of processing power of the bots and their internet connection speed.

DomingoVerdad - June 26, 2021, 11:25 am

Do you have to write the code yourself or are there good software packages for this "DDOS'ing for Dummies" sort of thing

guardian - June 26, 2021, 11:42 am

DDoS botnets need to have versatile techniques built in, in order to be 'powerful'. Depending on the target different types of attacks will be needed. Sometimes you will go with lower layers, sometimes with higher layers. Sometimes you will be facing certain types of protections (cloudflare, layer 3 firewall), which will need workarounds. The more situations the botnet is prepared for, the more attacks will succeed, which makes the botnet more powerful.