MY SUBREDDITS FRONT - ALL - RANDOM | ASKREDDIT - FUNNY - PICS - WORLDNEWS - GIFS - TODAYILEARNED - VIDEOS - GAMING - NEWS - AWW - MOVIES - SHOWERTHOUGHTS - IAM MORE »

DREADISCOOL overview comments submitted gilded

Want to join? Log in or sign up in seconds. | English

sorted by: **new**

Has anyone else seen an increase in ping lately? by **rutgerstemp9898** in rutgers
[–] **dreadiscool** 4 points 1 year ago

All traffic is being routed through Incapsula as of Tuesday morning last week
http://bgp.he.net/AS46

permalink context full comments (6)

1 Modern technology in the Avatar universe? (self.TheLastAirbender)
submitted 1 year ago by dreadiscool to /r/TheLastAirbender
1 comment share

Admission revoked?? by **Ilyminho** in rutgers
[–] **dreadiscool** 5 points 1 year ago

As long as you graduate they don't care

permalink context full comments (10)

@ogexfocus is back by **iaintevemaddy** in rutgers
[–] **dreadiscool** 2 points 1 year ago

They're peered with Incapsula and Level3 simultaneously, I suspect Incapsula is for ingress and Level3 for egress

permalink context full comments (44)

Hey everyone, I need YOUR help to get me into the next stage of my internship! It will benefit you as well, I promise! All you have to do is comment your email address by **[deleted]** in rutgers
[–] **dreadiscool** 4 points 1 year ago

Nope, please take your obvious ploy for attention for your new service elsewhere. It's not wanted here

permalink context full comments (3)

@ogexfocus is back by **iaintevemaddy** in rutgers
[–] **dreadiscool** 3 points 1 year ago

It's most likely miscommunication between the two departments. The university students are pressuring the administration to get things fixed. In turn, the administration is pressuring the IT department to get things fixed. There's really nothing they can do, but when they see a window of light (1 hour of uptime), they tell the administration that the problem is resolved, in fear of losing their jobs. As a result, the

dreadiscool

95 post karma
117 comment karma

✉ send a private message redditor for 1 year

TROPHY CASE what's this?

One-Year Club

Verified Email

briankrebs ••••••••••••

□ remember me reset password login

administration makes the wrong call and opens up webreg, and what a poop storm that was.....

permalink context full comments (44)

@ogexfocus is back by iaintevemaddy in rutgers
[–] dreadiscool 3 points 1 year ago

The way that tcptraceroute works is it uses SYN packets. So you need to specify the port of the target service you're tcptracerouting to. If the compsci website is only http, you have to use -p 80. If it's https, you have to do -p 443

permalink context full comments (44)

Flair here! Getcha flair here! by ANBU_Spectre in rutgers
[–] dreadiscool 1 point 1 year ago

COMPSCI

permalink context full comments (186)

@ogexfocus is back by iaintevemaddy in rutgers
[–] dreadiscool 5 points 1 year ago

Afaik Incapsula has has transit from Level 3. A few hours ago, you could see the Incapsula hop on there. I'm not sure if they dropped Incapsula, or if they just hid the hop.

If you have a Linux machine, try running tcptraceroute -p 80 <comp sci website>

Tcptraceroutes offer a better view of the path packets take by revealing hops that normally try to disguise themselves :D

permalink context full comments (44)

Rutgers IT updates are the worst by thebruns in rutgers
[–] dreadiscool 0 points 1 year ago

Implying that the attacker needed any information to pwn Rutgers? He's doing well enough without it...

permalink context full comments (22)

@ogexfocus is back by iaintevemaddy in rutgers
[–] dreadiscool 9 points 1 year ago

Exactly, DDoS mitigation isn't really a viable option for a university that uses the internet in many diverse ways. The solution is to just tank the attacks by absorbing the excess traffic

permalink context full comments (44)

Wifi hacked again? by Jamesified in rutgers
[–] dreadiscool 1 point 1 year ago

So you had it filtered all the way upstream to the home router that the attack was being generated from? waow

permalink context full comments (100)

Wifi hacked again? by Jamesified in rutgers
[–] dreadiscool 1 point 1 year ago*

I don't even have a response to that...

"The MAC addresses I was getting hit with were from brazil and russia" Just ...... MAC addresses operate at a layer 2 level. Let's say we have a packet

User MAC: 00:...

They use their router as a gateway. The router's MAC is 01:....

Let's say there are 3 hops in between the router and Facebook.

So the path that data travels in order to reach Facebook is

User <-> Router <-> Hop1 <-> Hop2 <-> Hop3 <-> Facebook

Facebook will never see the MAC address of the user, router, hop1, or hop2. Facebook will **only** see the MAC address of Hop3, because it is connected directly to Hop3. By filtering MAC addresses, you have just blocked one of the people who provide you internet connectivity. You aren't blocking the MAC address of the user at all.

Furthermore, are you sure you know what a botnet is? "They'll use a server farm in some weird country where power is extremely cheap". Botnets (usually) run on home computers, not on servers.

Furthermore, your claim of "30 routers being used to send the traffic" is an extremely low number. I think instead of routers, you meant ISPs.

tl;dr: The mac address you see are not the mac addresses of the machine that actually sent you traffic - it's the mac address of the machine that RELAYED you the traffic. Ethernet frames are not sent over the public internet, that's what the IP header is for.

That means that if you're behind a router, good ol' NAT, the only MAC address you will ever see is your router's MAC address. In turn, your router will only ever see the MAC addresses of the ISP.

permalink **context** **full comments (100)**

Wifi hacked again? by **Jamesified** in rutgers
[–] **dreadiscool** 1 point 1 year ago

A botnet has tens of thousands of IPs. If you were trying to do something like query a database (MaxMind) to find out the country of origin, think about what 40m queries might do to the database, especially if it was running on core routers... The query would have to be run for each packet that came through. It's not even possible to do it on most core routers as they use ASIC chips and do not support this kind of extendability.

Furthermore, MAC address filtering would not be reliable whatsoever. The reason you only got 4 - 5 mac addresses was because the MAC addresses you receive are the addresses of the routers/machines you're peered with, not the MAC addresses of the attacker's computers.

permalink **context** **full comments (100)**

Wifi hacked again? by **Jamesified** in rutgers
[–] **dreadiscool** 1 point 1 year ago

So tell me, how would you go about dropping traffic from only specific countries? That would be several hundred rules to push upstream. Zayo is extremely strict and doesn't allow upstream rules. Even more "liberal" providers will let you push at most 10...

permalink **context** **full comments (100)**

Wifi hacked again? by **Jamesified** in rutgers
[–] **dreadiscool** 1 point 1 year ago

Then we're back at issue #1. There are up to 50k people on campus, all using the internet for various different things. It is going to be very hard to push a rule that won't adversely affect some of the population.

permalink **context** **full comments (100)**

Wifi hacked again? by **Jamesified** in rutgers
[–] **dreadiscool** 3 points 1 year ago

If it's a botnet, there are tens of thousands of IPs - it's not prudent to block them all at Zayo's edge, or there will be service degradation while processing even regular traffic.

Also, the MAC address used in ethernet frames are for layer 2 purposes only - If you run a traceroute, the MAC address is (usually) from the hop right above you. You can't get someone's MAC address from the public internet unless you can send traffic to them directly (no hops in between you)

permalink **context** **full comments (100)**

Wifi hacked again? by **Jamesified** in rutgers
[–] **dreadiscool** 3 points 1 year ago*

No, unfortunately that is not how it works. You still haven't addressed point #2 and continue to restate your incorrect thoughts.

1) The Rutgers internet service is getting attacked. That means that 99% of traffic starts off as egress (initiating a connection). Clients pick a port number randomly. By blocking port numbers in an effort to stop a DDoS attack, you will be causing issues

2) Just because you have a rule to block a packet does not mean that the packet does not arrive at your network. Here's an example for you:

Let's say, for simplicity's sake, that the router is able to handle 10 packets per second. The attack signature is easily identifiable The attacker is now sending 11 packets per second. In order to identify if the packet is good or bad, the router must process it. Since the router can only process 10 packets per second, **it doesn't matter how well you detect the attack or detect IP addresses for being malicious**

You say "this allows the admin to block IPs the attack was coming from". If the Rutgers team has to implement ingress filtering at their network edge, it is too little too late. Let's change your analogy slightly: Instead of a fire hose and garden hose, let's use a highway and an exit.

Zayo is the highway - they mantain a large backbone and transport large amounts of traffic over their infrastructure regularly. Rutgers pays for an exit off the Zayo highway. Rutgers sees that they are getting a HUGE amount of cars in their exit, so they decide, in accordance with your logic, to place a security checkpoint on their exit (the firewall). Now even if the firewall rejects all packets, this does not stop the cars from attempting to queue into Rutgers' network. The offramp ahead of the security checkpoint is still saturated, and traffic is spilling onto the highway itself.

According to another post on here, Zayo itself was nullrouting Rutgers. That means that Zayo determined that the backlog of cars was so large that it was causing traffic jams on the highway itself, not just for people waiting to take the exit. Therefore, Zayo has put signs up at all **entrances** to their highway that Rutgers is not available - therefore, traffic will never reach Rutgers because it never gets on the Zayo highway.

You may ask "Why can Zayo not implement this for all 999999 IPs being used in the attack?" The answer is simple - routers are not fast enough to check each packet against that many rules, even with the ASIC chips inside of them. If Zayo did it for Rutgers, other organizations would ask for it too, and Zayo's network quality would suffer.

In short, you do seem to have some knowledge of how the Internet works, but you seem to be mistaken in thinking that blocking an IP address or closing a port will have any effect whatsoever in the resolution of these attacks.

Furthermore, what was the purpose of you specifying "ethernet frames"? An ethernet frame is just a packet at the layer 2 level. Since it is a packet, it would have been more prudent to call it a packet anyway. Another reason you may have mentioned it is you mistakenly thought that the MAC address contained in the ethernet frame would be the MAC address of the sender, and not of the router that acted as a hop in between. The other explanation would be you said ethernet frame just to be pedantic and sound smart :)

Edit 2: Even furthermore, even if the router is overloaded, it will not "freeze up" as you say - most modern routers and switches (aka the equipment Rutgers is most likely using) are more than capable of setting processor affinity, which means processes related to administration of the router/switch take a higher priority than the packet processing itself. That is, assuming that it is a software router (most likely it is not). In the case of a router using an ASIC chip (and therefore hardware packet processing), there is no chance whatsoever that overloading the ASIC chip would affect the administrative control. Since there is no chance that the packet processing part of the router/switch could affect the administrative controls, why do you even bring up disconnecting the router as a solution? You bringing up that solution makes me think you've only dealt with hardware >10 years old

permalink **context** **full comments (100)**

Wifi hacked again? by **Jamesified** in rutgers

[–] **dreadiscool** 8 points 1 year ago

"No one sends packets filled over 1gb of data." The MTU for most networks doesn't exceed 1500 bytes. Therefore, a packet can never exceed 1500 bytes in length. A packet 1gb in length? uw0tm8?

"All you have to do is set a rule to now allow over a certain size and that method is toast" Not if the routers ingress port is saturated - more traffic is coming in than it can handle. It doesn't matter if you block it - that traffic is hitting your router.

"Firewalls and routers just arent meant to handle massive amount of connections" Of course they aren't, they operate at the layer 3 level. This means they deal with packets only - they aren't concerned with connections, and most do not even have a conntable (except for use with the admin interface).

I understand you are trying to show off your knowledge here. But when it is so wrong, I would suggest you do some research before you post it online... Your arguments are fundamentally flawed.

permalink **context** **full comments (100)**

Wifi hacked again? by **Jamesified** in rutgers
[–] **dreadiscool** 0 points 1 year ago

Wowe Cloudflare I'm sure they will be useful for mitigating all the traffic that isn't HTTP

permalink **context** **full comments (100)**

Wifi hacked again? by **Jamesified** in rutgers
[–] **dreadiscool** 5 points 1 year ago

I don't understand why you're giving kudos to him for figuring out which IPs to attack - this information is all public and easily accessible

permalink **context** **full comments (100)**

Wifi hacked again? by **Jamesified** in rutgers
[–] **dreadiscool** 12 points 1 year ago*

You clearly have never dealt with situation #2 lol.

As someone whose product has been on the receiving end of a 310gbit/s unamplified DDoS attack and writes DDoS mitigation software, that solution doesn't work when your inbound port is saturated.

It doesn't matter if you block the IPs or not, because by the time you're inspecting the IP header it's too late - the packet has already arrived at your network. Even with a team of trained monkeys watching ingress traffic and blacklisting traffic, that doesn't change the fact that if your ingress port is saturated, you will go down - period.

Furthermore, what does unplugging the ingress link have to do with anything? You're helping the attacker by taking the services offline yourself...

permalink **context** **full comments (100)**

Wifi hacked again? by **Jamesified** in rutgers
[–] **dreadiscool** 1 point 1 year ago

I'm currently in Starbucks using what limited bandwidth I can scrape from my data plan... Is the internet back on campus yet?

permalink **context** **full comments (100)**

Wifi hacked again? by **Jamesified** in rutgers
[–] **dreadiscool** 18 points 1 year ago

There are two issues with that.

1) How do you determine "good" traffic from "bad" traffic? Tens of thousands of people use the internet here... If your rules are too strict, you will cause a great deal of harm to the people trying to use the internet.

2) The best filters and firewalls in the world won't work if they are simply overloaded - if the firewall is connected to a 40 gig line at the edge of Rutgers' network, and there's 41gbps of traffic coming to it, no amount of clever tricks will stop you from going down

permalink **context** **full comments (100)**

ELI5 why when you try to load a part of a video that isn't buffered, it'll lose all the buffered parts. by **Megaprr** in explainlikeimfive
[–] **dreadiscool** 1 point 1 year ago

They don't buffer the entire video though. Not unless the clip is something like 30 seconds

permalink **context** **full comments (5)**

view more: **‹ prev** | **next ›**

about
blog
about
source code
advertise
jobs

help
site rules
FAQ
wiki
reddiquette
transparency
contact us

apps & tools
Reddit for iPhone
Reddit for Android
mobile website
buttons

<3
reddit gold
redditgifts

π