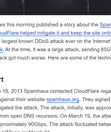
The DDoS That Almost Broke the Internet

06/27/2013

Matthew Prince



The New York Times this morning published a story about the Spamhaus DDoS attack and how CloudFlare helped mitigate it and keep the site online. The Times calls the attack the largest known DDoS attack ever on the Internet. We wrote about the attack last week. At the time, it was a large attack, sending 85Gbps of traffic. Since then, the attack got much worse. Here are some of the technical details of what we've seen.

Growth Spurt

On Monday, March 18, 2013 Spamhaus contacted CloudFlare regarding an attack they were seeing against their website spamhaus.org. They signed up for CloudFlare and we quickly mitigated the attack. The attack, initially, was approximately 10Gbps generated largely from open DNS recursors. On March 19, the attack increased in size, peaking at approximately 90Gbps. The attack fluctuated between 90Gbps and 300Gbps until 01:15 UTC on March 21.

The attackers were quiet for a day. Then, on March 22 at 18:00 UTC, the attack resumed, peaking at 120Gbps of traffic hitting our network. As we discussed in the previous blog post, CloudFlare uses Anycast technology which spreads the load of a distributed attack across all our data centers. This allowed us to mitigate the attack without it affecting Spamhaus or any of our other customers. The attackers changed their attack against the Spamhaus website four hours after it started.

Other than the scale, which was already among the largest DDoS attacks we've seen, there was nothing particularly unusual about the attack to this point. Then the attackers changed their tactics. Rather than attacking our customers directly, they started going after the network providers CloudFlare uses for bandwidth. More on that in a second, first a bit about how the Internet works.

Peering on the Internet

The "Inter" in Internet refers to the fact that it is a collection of independent networks connected together. CloudFlare runs a network, Google runs a network, and bandwidth providers like Level3, AT&T, and Cogent run networks. These networks then interconnect through what are known as peering relationships.

When you surf the web, your browser sends and receives packets of information. These packets are sent from one network to another. You can see this by running a traceroute. Here's one from Stanford University's network to the New York Times' website (nytimes.com):

```
1  rtr-servcore1-serv01-ubdmzvl.slac.stanford.edu (134.79.187.198) 0.572 ms
2  rtr-inval-gigv-servcore1.slac.stanford.edu (134.79.252.166) 0.796 ms
3  rtr-bordervl-p2p-inval.slac.stanford.edu (134.79.252.133) 0.534 ms
4  sunncr5-ip-a-slacmr1.es.net (134.55.218.105) 1.040 ms 1.054 ms
5  sunncr5-ip-a-slacmr1.es.net (134.55.42.34) 1.386 ms
6  equin2r1-te-sunncr5.es.net (134.55.38.146) 1.384 ms
7  chic-cr5-ip-a-equin2r1.es.net (134.55.49.114) 49.415 ms
8  ne-96-0-0-ear1.newyork.level3.net (4.68.123.3)?  28.812 ms
9  209.244.112.125 (209.244.112.125)  31.985 ms
```

There are three networks in the above traceroute: stanford.edu, es.net, and above.net. The request starts at Stanford. Between lines 4 and 5 it passes from Stanford's network to their peer es.net. Then, between lines 6 and 7, it passes from es.net to above.net, which appears to provide hosting for the New York Times. This means Stanford has a peering relationship with ES.net. ES.net has a peering relationship with Above.net. And Above.net provides connectivity for the New York Times.

CloudFlare connects to a large number of networks. You can get a sense of some, although not all, of the networks we peer with through a tool like Hurricane Electric's BGP looking glass. CloudFlare connects to peers in two ways. First, we connect directly to certain large carriers and other networks to which we send a large amount of traffic. In this case, we connect our router directly to the router at the border of the other network, usually with a piece of fiber optic cable. Second, we connect to what are known as Internet Exchanges, IXs for short, where a number of networks meet in a central point.

Most major cities have an IX. The model for IXs are different in different parts of the world. Europe runs some of the most robust IXs, and CloudFlare connects to several of them including LINX (the London Internet Exchange), AMS-IX (the Amsterdam Internet Exchange), and DE-CIX (the Frankfurt Internet Exchange), among others. The major networks that make up the Internet —Google, Facebook Yahoo, etc.— connect to these same exchanges to pass traffic between each other efficiently. When the Spamhaus attacker realized he couldn't go after CloudFlare directly, he began targeting our upstream peers and exchanges.

Headwaters

Once the attackers realized they couldn't knock CloudFlare itself offline even with more than 100Gbps of DDoS traffic, they went after our direct peers. In this case, they attacked the providers from whom CloudFlare buys bandwidth. We, primarily, contract with what are known as Tier 2 providers for CloudFlare's paid bandwidth. These companies peer with other providers and also buy bandwidth from so-called Tier 1 providers.

There are approximately a dozen Tier 1 providers on the Internet. The nature of these providers is that they don't buy bandwidth from anyone. Instead, they engage in what is known as settlement-free peering with the other Tier 1 providers. Tier 2 providers interconnect with each other and then buy bandwidth from the Tier 1 providers in order to ensure they can connect to every other point on the Internet. At the core of the Internet, if all else fails, it is these Tier 1 providers that ensure that every network is connected to every other network. If one of them fails, it's a big deal.

Anycast means that if the attacker attacked the last step in the traceroute then their attack would be spread across CloudFlare's worldwide network. Second, we noticed they attacked the second to last step which concentrated the attack on one single point. This wouldn't cause a network-wide outage, but it could potentially cause regional problems.

We carefully select our bandwidth providers to ensure they have the ability to deal with attacks like this. Our direct peers quickly filtered attack traffic at their edge. This pushed the attack upstream to their direct peers, largely Tier 1 networks. Tier 1 networks don't buy bandwidth from anyone, so the majority of the weight of the attack ended up being carried by them. While we don't have direct visibility into the traffic loads they saw, we have been told by one major Tier 1 provider that they saw more than 300Gbps of attack traffic related to this attack. That would make this attack one of the largest ever reported.

The challenge with attacks at this scale is they risk overwhelming the systems that link together the Internet itself. The largest routers that you can buy have, at most, 100Gbps ports. It is possible to bond more than one of these ports together to create capacity that is greater than 100Gbps however, at some point, there are limits to how much these routers can handle. If that limit is exceeded then the network becomes congested and slows down.

Over the last few days, as these attacks have increased, we've seen congestion across several major Tier 1s, primarily in Europe where most of the attacks were concentrated, that would have affected hundreds of millions of people even as they surfed sites unrelated to Spamhaus or CloudFlare. If the Internet felt a bit more sluggish for you over the last few days in Europe, this may be part of the reason why.

Attacks on the IXs

In addition to CloudFlare's direct peers, we also connect with other networks over the so-called Internet Exchanges (IXs). These IXs are, at their most basic level, switches into which multiple networks connect and can then pass bandwidth. In Europe, these IXs are run as non-profit entities and are considered critical infrastructure. They interconnect hundreds of the world's largest networks including CloudFlare, Google, Facebook, and just about every other major Internet company.

Beyond attacking CloudFlare's direct peers, the attackers also attacked the core IX infrastructure on the London Internet Exchange (LINX), the Amsterdam Internet Exchange (AMS-IX), the Frankfurt Internet Exchange (DE-CIX), and the Hong Kong Internet Exchange (HKIX). From our perspective, the attacks had the largest effect on LINX which caused impact over the exchange and LINX's systems that monitor the exchange, as visible through the drop in traffic recorded by their monitoring systems. (Corrected: see below for original phrasing.)

The congestion impacted many of the networks on the IXs, including CloudFlare's. As problems were detected on the IX, we would route traffic around them. However, several London-based CloudFlare users reported intermittent issues over the last several days. This is the root cause of those problems.

The attacks also exposed some vulnerabilities in the architecture of some IXs. We, along with many other network security experts, worked with the team at LINX to better secure themselves. In doing so, we developed a list of best practices for any IX in order to make them less vulnerable to attacks.

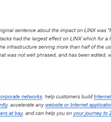
Two specific suggestions to limit attacks like this involve making it more difficult to attack the IP addresses that members of the IX use to interchange traffic between each other. We are working with IXs to ensure that: 1) these IP addresses should not be announced as routable across the public Internet; and 2) packets destined to these IP addresses should only be permitted from other IX IP addresses. We've been very impressed with the team at LINX and how quickly they've worked to implement these changes and add additional security to their IX and are hopeful other IXs will quickly follow their lead.

The Full Impact of the Open Recursor Problem

At the bottom of this attack we once again find the problem of open DNS recursors. The attackers were able to generate more than 300Gbps of traffic likely with a network of their own that only had access 11/10th of that amount of traffic themselves. We've written about how these mis-configured DNS recursors as a bomb-waiting to go off that literally threatens the stability of the Internet itself. We've now seen an attack that begins to illustrate the full extent of the problem.

While lists of open recursors have been passed around on network security lists for the last few years, on Monday the full extent of the problem was, for the first time, made public. The Open Resolver Project made available the full list of the 21.7 million open resolvers online in an effort to shut them down.

We'd debated doing the same thing ourselves for some time but worried about the collateral damage of what would happen if such a list fell into the hands of the bad people. The last five days have made clear that the bad people have the list of open resolvers and they are getting increasingly brazen in the attacks they are willing to launch. We are in full support of the Open Resolver Project and believe it is incumbent on all network providers to work with their customers to close any open resolvers running on their networks.



Unlike traditional botnets which could only generate limited traffic because of the modest Internet connections and home PCs they typically run on, these open resolvers are typically running on big servers with fat pipes. They are like bazookas and the events of the last week have shown the damage they can cause. What's troubling is that, compared with what is possible, this attack may prove to be relatively modest.

As someone in charge of DDoS mitigation at one of the Internet giants emailed me this weekend, "I've often said we don't have to prepare for the largest-possible attack, we just have to prepare for the largest attack the Internet can send without causing massive collateral damage to others. It looks like you've reached that point, so... congratulations!"

At CloudFlare one of our goals is to make DDoS something you only read about in the history books. We're proud of how our network held up under such a massive attack and are working with our peers and partners to ensure that the Internet overall can stand up to the threats it faces.

***Correction**: The original sentence about the impact on LINX was "From our perspective, the attacks had the largest effect on LINX which for a little over an hour on March 23 saw the infrastructure serving more than half of the usual 1.5Tbps of peak traffic fail." That was not well phrased, and has been edited, with notation in place.*

We protect entire corporate networks, help customers build Internet-scale applications efficiently, accelerate any website or Internet application, ward off DDoS attacks, keep hackers at bay, and can help you on your journey to Zero Trust.

Visit 1.1.1.1 from any device to get started with our free app that makes your Internet faster and safer.

To learn more about our mission to help build a better Internet, start here. If you're looking for a new career direction, check out our open positions.

Discuss on Hacker News

Reliability | DDoS | Attacks | Mitigation

Follow on Twitter

Matthew Prince | @eastdakota
Cloudflare | @Cloudflare

RELATED POSTS

July 06, 2022 1:55PM
DDoS attack trends for 2022 Q2
Welcome to our 2022 Q2 DDoS report. This report includes insights and trends about the DDoS threat landscape — as observed across the global Cloudflare network.
By Omer Yoachimik
DDoS, DDoS Reports, Attacks, Trends, Cloudflare Radar

April 12, 2022 2:12PM
DDoS Attack Trends for 2022 Q1
Welcome to our first DDoS report of 2022, and the ninth in total so far. This report includes new data points and insights both in the application-layer and network-layer sections — as observed across the global Cloudflare network between January and March 2022.
By Omer Yoachimik
DDoS, DDoS Reports, Attacks, Trends, Cloudflare Radar

January 10, 2022 1:58PM
DDoS Attack Trends for Q4 2021
In Q4, we observed a 95% increase in L3/4 DDoS attacks and record-breaking levels of Ransom DDoS attacks. The Manufacturing industry was the most targeted alongside a 5,800% increase in SNMP-based DDoS attacks and new campaigns against VoIP providers detected.
By Omer Yoachimik, Vivek Ganti
DDoS, Attacks, Trends, Cloudflare Radar, Ransom DDoS

April 25, 2017 8:45AM
Ecommerce websites on Cloudflare: best practices
Cloudflare provides numerous benefits to ecommerce sites, including advanced DDoS protection and an industry-leading Web Application Firewall (WAF) that helps secure your transactions and protect customers' private data.
By Nick B
eCommerce, Tips, Paper, Product, JavaScript

© 2022 Cloudflare, Inc. | Privacy Policy | Terms of Use | Trust & Safety | Trademark