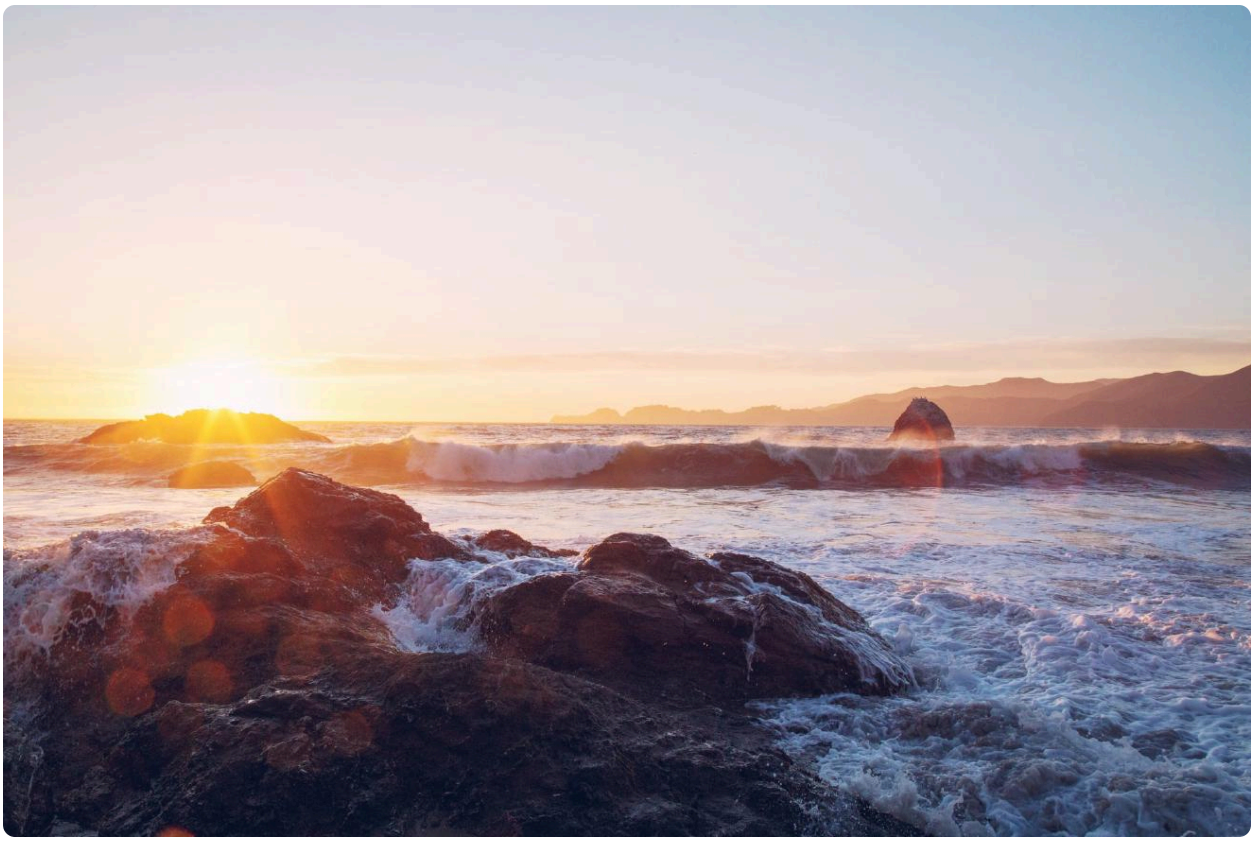
A new future for icanhazip



Sebastien Gabriel on Unsplash

In the summer of 2009, I had an idea. My workdays were spent deploying tons of cloud infrastructure as Rackspace acquired Slicehost and we rushed to keep up with the constant demands for new infrastructure from our customers. Working quickly led to challenges with hardware and networking.

That was a time where the I Can Has Cheeseburger meme was red hot just about everywhere. We needed a way to quickly check the public-facing IP address of lots of backend infrastructure and our customers sometimes needed that information, too.

That's when icanhazip.com was born.

It has always been simple site that returns your external IP address and nothing else. No ads. No trackers. No goofy requirements. Sure, if you looked hard enough, you could spot my attempt at jokes in the HTTP headers. Other than that, the site had a narrow use case and started out mainly as an internal tool.

That's when things got a little crazy

Lifehacker's Australian site featured a post about icanhazip.com and traffic went through the roof. My little Slicehost instance was inundated and I quickly realized my Apache and Python setup was not going to work long term.

I migrated to nginx and set up nginx to answer the requests by itself and removed the Python scripts. The load on my small cloud instances came down quickly and I figured the issue would be resolved for a while.

Fast forward to 2015 and icanhazip.com was serving well over 100M requests per day. My cloud instances were getting crushed again, so I deployed more with round robin DNS. *(My budget for icanhazip is tiny.)* Once that was overloaded, I moved to Hetzner in Germany since I could get physical servers there with better network cards along with unlimited traffic.

The Hetzner servers were not expensive, but I was paying almost $200/month to keep the site afloat and the site made no money. I met some people who worked for Packet.net (now Equinix Metal) and they offered to sponsor the site. This brought my expenses down a lot and I deployed icanhazip.com on one server at Packet.

The site soon crossed 500M requests per day and I deployed a second server. Traffic was still overloading the servers. I didn't want to spin up more servers at Packet since they were already helping me out quite a bit, so I decided to look under the hood of the kernel and make some improvements.

I learned more than I ever wanted to know about TCP backlogs, TCP/VLAN offloading, packet coalescing, IRQ balancing, and a hundred other things. Some Red Hat network experts helped me (before I joined the company) to continue tweaking. The site was running well after that and I was thankful for the support.

Even crazier still

Soon the site exceeded 1B requests per day. I went back to the people who helped me at Red Hat and after they looked through everything I sent, their response was similar to the well-known line from Jaws: *"You're gonna need a bigger boat."*

I languished on Twitter about how things were getting out of control and someone from Cloudflare reached out to help. We configured Cloudflare to filter traffic in f

the site and this reduced the impact from SYN floods, half-open TLS connections, and other malicious clients that I couldn't even see when I hosted the site on my own.

Later, Cloudflare launched workers and my contact there said I should consider it since my responses were fairly simple and the workers product would handle it well. The cost for workers looked horrifying at my traffic levels, but the folks at Cloudflare offered to run my workers for free. Their new product was getting bucket loads of traffic and I was able to scale the site even further.

In 2021, the traffic I once received in a month started arriving in 24 hours. The site went from 1B requests per day to 30-35B requests per day over a weekend. Almost all of that traffic came from several network blocks in China. Through all of this, Cloudflare's workers kept chugging along and my response times barely moved. I was grateful for the help.

Cloudflare was doing a lot for me and I wanted to curb some of the malicious traffic to reduce the load on their products. I tried many times to reach out to the email addresses on the Chinese ASNs and couldn't make contact with anyone. Some former coworkers told me that my chances of changing that traffic or getting a response to an abuse request was near zero.

Malware almost ended everything

There was a phase for a few years where malware authors kept writing malware that would call out to icanhazip.com to find out what they had infected. If they could find out the external IP address of the systems they had compromised, they could quickly assess the value of the target. Upatre was the first, but many followed after that.

I received emails from companies, US state governments, and even US three letter agencies (TLA). Most were very friendly and they had lots of questions. I explained how the site worked and rarely heard a lot more communication after that.

Not all of the interactions were positive, however. One CISO of a US state emailed me and threatened all kinds of legal action claming that icanhazip.com was involved in a malware infection in his state's computer systems. I tried repeatedly to explain how the site worked and that the malware authors were calling out to my site and I was powerless to stop it.

Along the way, many of my hosting providers received abuse emails about the site. I was using a colocation provider in Dallas for a while and the tech called me about an abuse email:

> *""So we got another abuse email for you," they said.*
>
> *"For icanhazip.com?"*
>
> *"Yes. I didn't know that was running here, I use it all the time!"*
>
> *"Thanks! What do we do?"*
>
> *"Your site just returns IP addresses, right?"*
>
> *"Yes, that's it."*
>
> *"You know what, I'll write up a generic response and just start replying to these idiots for you from now on.""*

There were many times where I saw a big traffic jump and I realized the traffic was coming from the same ASN, and likely from the same company. I tried reaching out to these companies when I saw it but they rarely ever replied. Some even became extremely hostile to my emails.

The passion left in my passion project started shrinking by the day.

The fun totally dried up

Seeing that over 90% of my traffic load was malicious and abusive was frustrating. Dealing with the abuse emails and complaints was worse.

I built the site originally as just a utility for my team to use, but then it grew and it was fun to find new ways to handle the load without increasing cost. Seeing 2 petabytes of data flowing out per month and knowing that almost all of it was garbage pushed me over the line. I knew I needed a change.

I received a few small offers from various small companies ($5,000 or less), but I realized that the money wasn't what I was after. I wanted someone to run the site and help the information security industry to stop some of these malicious actors.

icanhazip.com lives on at Cloudflare

I've worked closely with my contacts at Cloudflare for a long time and they've always jumped in to help me when something wasn't working well. Their sponsorship of icanhazip.com has saved me tens of thousands of dollars per month. It has also managed to keep the site alive even under horrific traffic load.

I made this decision because Cloudflare has always done right by me and they've pledged not only to keep the site running, but to work through the traffic load and determine how to stop the malicious traffic. Their coordinated work with other companies to stop compromised machines from degrading the performance of so many sites was a great selling point for me.

If you're curious, Cloudflare did pay me for the site. We made a deal for them to pay me $8.03; the cost of the domain registration. The goal was never to make money from the site (although I did get about $75 in total donations from 2009 to 2021). The goal was to provide a service to the internet. Cloudflare has helped me do that and they will continue to do it as the new owners and operators of icanhazip.com.

Gratitude

I'd like to thank everyone who has helped me with icanhazip.com along the way. Tons of people stepped up to help with hosting and server optimization. Hosting providers helped me field an onslaught of abuse requests and DDoS attacks. Most of all, thanks to the people who used the site and helped to promote it.

Photo credit: Sebastien Gabriel on Unsplash