8chan is all the way down—“It’s DNS. It’s always DNS.”

“Look, just host our website. It’ll be fine, we promise.”

reader comments

156 with 101 posters participating, including story author

Share this story

Earlier today in the Ars Technica staff Slack channel, a call went out—”is 8chan down for other people? I can’t get it to load anymore.” This brings up the interesting question of how to check where and why a site might be down, as well as whether it can even load for anyone.

But first a little background.

When Cloudflare finally had enough of 8chan and fired it, the site—notoriously a haven for mass shooters and their fans—immediately jumped ship for BitMitigate, the same CDN that hosts far-right white nationalist site The Daily Stormer. The site also changed DNS and Web hosting to Epik, which is the parent company to BitMitigate and the host of far-right social media platform Gab.

Alex Stamos, cybersecurity expert at Stanford University and former CSO of Facebook, observed that BitMitigate seemed itself to be almost entirely made of equipment and network infrastructure leased from a company called Voxility. This public and pointed observation prompted Voxility to fire BitMitigate and Epik, leaving both 8chan and The Daily Stormer

dead in the water.

This brings us back to the lede: when a site is dead, how can you figure out why it's dead and whether it's likely to be dead for everybody or just for yourself? If you have access to a Linux, FreeBSD, or Mac computer—or to the Windows Subsystem for Linux—answering these questions is not too difficult. The first thing to realize is that you need DNS in order to have a website.

The most important troubleshooting tool for DNS is a command-line utility called **dig**. Dig allows you to query DNS records directly; it's sort of like **nslookup** on steroids. By default, just like **nslookup**, **dig** will query whatever your locally configured DNS server is. But you can ask it to query any arbitrary server directly, and you can ask it for exactly the records you want.

- Starting out simple: we just want to know what the nameserver(s) for 8ch.net is so we can query one directly. Standard DNS infrastructure failed us; so we'll need to dig deeper.
  Jim Salter
- The parent domain of 8ch.net is, well, net. So, what are the DNS servers for the net TLD? And do they know where 8ch.net's DNS servers should be?
  Jim Salter
- Now that we've found the glue records for 8ch.net's DNS servers, let's try querying them directly. Looks like they don't want to talk.
  Jim Salter
- Last-gasp check on 8ch.net's DNS servers: are they even responding on port 53 at all? Nmap's "filtered" response means that there may or may not be a machine there—but it's not talking to us, regardless.
  Jim Salter

If you follow through the gallery above, what we're doing should be reasonably clear. First, we query our standard DNS infrastructure, asking it where to find a nameserver for 8ch.net—and we come up empty: our own local DNS server hasn't the foggiest clue.

The next step starts to get a bit more wizardly—we know that **8ch.net** is a subdomain of the top-level domain **net**. So, we ask for the nameserver for **net** itself—and armed with an answer, we can directly query a root nameserver for information about **8ch.net**'s DNS infrastructure. **a.gtld-servers.net** tells us that the DNS for **8ch.net** is handled by **ns2.8ch.net** and **ns3.8ch.net**. It offers us glue records so that we can reach them.

Once we start asking questions from **ns2.8ch.net** and **ns3.8ch.net**, we quickly discover that they aren't answering any questions at all. So, that's that—**8ch.net** cannot possibly be up, because the domain itself isn't answering any DNS queries. Even if the Web servers and database servers are functional, there's no way to *find* them.

We can still learn more, though. We know that Epik, the hosting service that owns BitMitigate and is supposed to be providing hosting for 8chan and The Daily Stormer, is still online despite having its own netblock cancelled by Voxility. Why would that be?

- A quick wget confirms that a Web server is answering and operational for epik.com itself. Hmm. OK, where are *its* nameservers, then…?
  Jim Salter
- When we use the **whois** command to check the netblocks of the three actual DNS servers handling the epik.com domain, we see they're hosted at Linode, Amazon, and OVH.
  Jim Salter
- Using the same technique, we can find the IP address of

> Epik's webserver and see whose netblock it's hosted on.
> Jim Salter

The **dig** command served us well in terms of finding DNS information by walking up and down the DNS hierarchy. But in order to figure out why Epik's own DNS is working despite its network infrastructure being down, we turn to the **whois** command. (I've piped the results through grep in order to show only the information I'm looking for; otherwise, the wealth of data returned wouldn't fit on one screen.) The whole process looks like this:

1. **dig +short NS epik.com** to get the hostnames of its nameservers
2. **dig +short A** each of the hostnames from step one, to get raw IP addresses
3. Pipe that whole mess through **sort -nu** so that we only get one return for each individual IP address serving DNS for epik.com
4. Finally, we can start using **whois** on those IP addresses to see whose netblocks they're hosted in.

In the screenshot gallery, you can see I've piped the **whois** results through **grep** for OrgName. This isn't strictly necessary, but **whois** by itself returns pages of information; **grep** allows us to only look at the lines containing keyword OrgName—which is the organization responsible for managing the subnet of IP addresses they're each in. This nets us one IP address at Linode, another at Amazon Web Services, and the third at OVH, a large European cloud provider. (We can also find that Epik's website itself is running on a Web server hosted at NatCoWeb, a New Jersey-based hosting provider.)

We can also take a look at the **whois** information for the netblock containing 8ch.net's DNS servers and The Daily Stormer's Web server. Epik's now-disconnected netblock is in Switzerland, so we need to query RIPE's infrastructure rather than ARIN's, and the format is a little different—but we can

see that it’s registered to Robert Monster, the CEO of Epik and BitMitigate. (There is a contact address and phone number for Monster listed in Sammamish, Washington. We tried calling but received no answer; the number went to a generic voicemail with no configured greeting.)

What this all boils down to is that Epik itself only seems “up” because Epik—unlike 8chan and The Daily Stormer—isn’t hosted on Epik at all.

https://arstechnica.com/?p=1546157