New Cloudflare tool can tell you if your ISP has deployed BGP fixes

Tommy Lee Walker | Getty Images

reader comments

63 with 51 posters participating

Share this story

For more than an hour at the beginning of April, major sites like Google and Facebook sputtered for large swaths of people. The culprit wasn’t a hack or a bug. It was problems with the internet data routing standard known as the Border Gateway Protocol, which had allowed significant amounts of web traffic to take an unexpected detour through a Russian telecom. For Cloudflare CEO Matthew Prince, it was the last straw.

BGP disruptions happen frequently, generally by accident. But BGP can also be hijacked for large-scale spying, data interception, or as a sort of denial of service attack. Just last week, United States Executive Branch agencies moved to block China Telecom from offering services in the US, because of allegedly malicious activity that includes BGP attacks. Companies like Cloudflare sit on the front lines of the BGP blowback. And while the company can’t fix the problem directly, it can call out those that are slow to contribute defenses.

On Friday, the company launched Is BGP Safe Yet, a site that makes it easier for anyone to check whether their internet service provider has added the security protections and filters that can make BGP more stable. Those improvements are most effective with wide adoption from ISPs, content delivery networks like Cloudflare, and other cloud providers. Cloudflare estimates that so far about half of the internet is more protected thanks to heavy hitters like AT&T, the Swedish telecom Telia, and the Japanese telecom NTT adopting BGP improvements. And while Cloudflare says it doesn't seem like the Rostelecom incident was intentional or malicious, Russian telecoms do have a history of suspicious BGP meddling, and similar problems will keep cropping up until the whole industry is on board.

"With that last big route leak from a few weeks ago out of Russia it was a point at which our engineering team said enough is enough, it's time for us to start naming and shaming the companies who aren't doing this right," says Cloudflare CEO Matthew Prince. "Anything that goes wrong anywhere on the internet we get blamed for it, which is right! Our customers pay us to make sure their internet connections are fast and secure and reliable. So BGP is one of these really frustrating areas that we can't solve ourselves."

BGP is like a GPS mapping service for the internet, enabling ISPs to automatically choose what route data should take over the internet's vast landscape of networks. But really BGP is like using a GPS mapping service run by your opinionated relatives. Your cousin's step-father says "oh, take *this* route. It'll be fast and safe and you get to pass the house with the great Halloween decorations," and you just have to trust him. If he doesn't know what he's talking about—like an ISP advertising a bad BGP route—you could end up stuck in endless mall traffic.

The cryptographic tools, route filters, and best practices Cloudflare and other organizations have been promoting are

like a sixth sense for detecting when you're getting bad advice. They run actual checks on the BGP routes other IPs are "announcing," or offering, to make sure they're legitimate and that no one is advertising a problematic route.

Is BGP Safe Yet will test your ISP by offering a legitimate route and an invalid one to load two pages. If your ISP catches the invalid route and only loads the page on the real route, it passes the test. But if it accepts both routes as valid, your ISP will fail, meaning that it hasn't yet implemented the BGP protections to check for bad routes and filter them.

Even with a large number of services still not offering BGP protections, you can still reap benefits from those that do. Prince explains that during a disruption like the Russian telecom incident, ISPs using BGP best practices would identify the issue, often called a "route leak," and reject it in favor of a legitimate route. So if your home Wi-Fi comes from Comcast, which hasn't yet implemented the improvements, and you get your mobile data from AT&T, which has, you might have issues loading certain websites and services on your laptop during a BGP incident, but could access them fine from your smartphone.

You probably don't have a direct line to the CEO of your ISP to complain about its lack of hustle on BGP protections. Cloudflare hopes, though, that the tool will raise awareness among consumers while also providing an easy way for industry players to see and be seen.

"BGP is a 40-plus-year-old protocol, it's a miracle the internet has worked on what is really just a trust-based system for as long as it has," Prince says. "Obviously it makes sense to have more verification, because anything else is madness. And yet! It's taken a long time to actually get that implemented. Hopefully we can put a little bit of public pressure on."

This story originally appeared on wired.com.

https://arstechnica.com/?p=1669279