Nigerian ISP's configuration error disrupted Google services

November 13 2018, by Frank Bajak

In this Monday, Nov. 5, 2018, photo, a woman carries a fire extinguisher past the logo for Google at the China International Import Expo in Shanghai. Internet traffic hijacking disrupted several Google services Monday, Nov. 12, 2018, including search and cloud-hosting services. (AP Photo/Ng Han Guan)

A Nigerian internet service provider said Tuesday that a configuration error it made during a network upgrade caused a disruption of key Google services, routing traffic to China and Russia.

Prior to MainOne's explanation Tuesday, there was speculation that Monday's 74-minute data hijacking might have been intentional. Google's search, cloud hosting and collaborative business tools were among services disrupted.

"Everyone is pretty confident that nothing untoward took place," MainOne spokeman Tayo Ashiru said.

The type of traffic misdirection involved can knock essential services offline and facilitate espionage and financial theft. They can also be used to block access to information by sending data into internet black holes. Experts say China, in particular, has systematically hijacked and diverted U.S. internet traffic.

But the problem can also result from human error. That's what Ashiru said happened to MainOne, a major west African ISP. He said engineers mistakenly forwarded to China Telecom addresses for Google services that were supposed to be local. The Chinese company, in turn, sent along the bad data to Russia's TransTelecom, a major internet presence. Ashiru said MainOne did not yet understand why China Telecom did that, as the state-run company normally doesn't allow Google traffic on its network.

The traffic diversion into China created a detour with a dead end, preventing users from accessing the affected Google services, said Alex Henthorn-Iwane, an executive at the network-intelligence company ThousandEyes.

He said Monday's incident offered yet another lesson in the internet's susceptibility to "unpredictable and destabilizing events. If this could happen to a company with the scale and resources available that Google has, realize it could happen to anyone."

The diversion, known as gateway protocol hijacking, is built into the internet, which was designed for collaboration by trusted parties—not competition by hostile nation-states. Experts say it is fixable but that would require investments in encrypted routers that the industry has resisted .

ThousandEyes said the diversion at minimum made Google's search and business collaboration tools difficult or impossible to reach and "put valuable Google traffic in the hands of ISPs in countries with a long history of Internet surveillance."

However, most network traffic to Google services—94 percent as of Oct. 27—is encrypted, which shields it from prying eyes even if diverted. Google said in a statement that "access to some Google services was impacted" but did not further quantify the disruption.

Google said it had no reason to believe the traffic hijacking was malicious.

Indeed, the phenomenon has occurred before. Google was briefly afflicted in 2015 when an Indian provider stumbled. In perhaps the best-known case, Pakistan Telecom inadvertently hijacked YouTube's global traffic in 2008 for a few hours when it was trying to enforce a domestic ban. It sent all YouTube traffic into a virtual ditch in Pakistan.

In two recent cases, such rerouting has affected financial sites. In April 2017, one affected MasterCard and Visa among other sites. This past April, another hijacking enabled cryptocurrency theft .

Citation: Nigerian ISP's configuration error disrupted Google services (2018, November 13) retrieved 26 April 2024 from
https://phys.org/news/2018-11-nigerian-isp-error-disruption-google.html