Internet traffic hijack disrupts 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)

An internet traffic diversion rerouted data through Russia and China and disrupted Google services on Monday, including search, cloud-hosting services and its bundle of collaboration tools for businesses.

Service interruptions lasted for nearly one and a half hours and ended about 5:30 p.m. EST., network service companies said. In addition to Russian and Chinese telecommunications companies, a Nigerian internet provider was also involved.

The diversion "at a minimum caused a massive denial of service to G Suite (business collaboration tools) and Google Search" and "put valuable Google traffic in the hands of ISPs in (internet service providers) in countries with a long history of Internet surveillance," the network-intelligence company ThousandEyes said in a blog post.

A Google status page noted that "access to some Google services was impacted" and said the cause was "external to Google ." The company offered little additional information.

The type of traffic misdirection employed, known as border gateway protocol hijacking, can knock essential services offline and facilitate espionage and financial theft. It can result either from misconfiguration—human error, essentially— or from malicious action.

Most network traffic to Google services —94 percent as of October 27—is encrypted, which shields it from prying eyes even if diverted.

Alex Henthorn-Iwane, an executive at ThousandEyes, called Monday's incident the worst affecting Google that his San Francisco company has seen.

He said he suspected nation-state involvement because the traffic was effectively landing at state-run China Telecom. A recent study by U.S. Naval War College and Tel Aviv University scholars found that China systematically hijacks and diverts U.S. internet traffic.

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

malicious. It did not explain why.

Much of the internet's underpinnings are built on trust, a relic of the good intentions its designers assumed of users. One consequence: little can be done if a nation-state or someone with access to a major internet provider—or exchange—decides to reroute traffic.

Henthorn-Iwane says Monday's hijacking may have been "a war-game experiment."

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 .

The Department of Homeland Security did not immediately respond to a request for comment.

ThousandEyes named the companies involved in Monday's incident, in addition to China Telecom, as the Russian internet provider Transtelecom and the Nigerian ISP MainOne.

Both ThousandEyes and the U.S. network monitoring company BGPmon said the internet traffic detour originated with the Nigerian company. Neither was ready to more definitively pinpoint the cause.