Issued 11/13/18

Google Went Down after Traffic was Routed through China and Russia

Google's services went down for an hour yesterday after its IP addresses were routed way from normal paths to Nigeria, China and Russia. Google told Ars Technica it doubted the leak was malicious, despite the fact that government-owned China Telecom was recently caught routing Western carrier traffic through mainland China. Some of Google's most sensitive data, including its corporate WAN infrastructure and VPN, were reportedly redirected. The problem started when a carrier in Lagos, Nigeria improperly declared its own system as the correct route to several hundred IP prefixes belonging to Google. China Telecom accepted the route (also improperly) and declared it worldwide. That in turn was picked up by Russia's Transtelecom and other large ISP services. Later on, the same Nigerian carrier made a second incorrect IP declaration that sent Google partner Cloudflare's IP addresses on a similar joyride. This incident at a minimum caused a massive denial of service to G Suite and Google Search. However, this also put valuable Google traffic in the hands of ISPs in countries with a long history of Internet surveillance. Overall ThousandEyes detected over 180 prefixes affected by this route leak, which covers a vast scope of Google services. Google said that its services weren't compromised because almost all of its traffic is encrypted. (Facebook also experienced a rare outage yesterday that was reportedly unrelated.) It's a reminder of how sensitive global internet protocols heavily rely on trust, something that's lacking in today's climate of online spying, election

hacking, cryptocurrency theft and other major issues. "This incident put valuable Google traffic in the hands of ISPs in countries with a long history of Internet surveillance."