Glitch diverts net traffic through Chinese ISP

Twice in two weeks

By Dan Goodin in San Francisco

Posted in Security, 10th April 2010 07:02 GMT

Free whitepaper – Intel Xeon processor 7500 series ROI brief

Internet service providers in China briefly tainted network routing tables on Thursday, marking the second time in two weeks operators in that country have done so, IDG news reports (http://www.computerworld.com/s/article/9175081/A_Chinese_ISP_momentarily_hijacks_the_Internet_again_).

The bad networking information originated from IDC China Telecommunication and was soon retransmitted by China's state-owned China Telecommunications. ISPs including AT&T, Level3, Deutsche Telekom, Qwest Communications and Telefonica soon incorporated the data into their tables as well, IDG said.

As a result, routing information for 32,000 to 37,000 networks was affected, potentially causing them to be redirected through IDC China instead of their path. Some 8,000 of the networks were located in the US, including those operated by Dell, Apple, CNN, and Starbucks. Networks in Australia, China and elsewhere were also affected.

The incident comes two weeks after a similar networking anomaly caused people in Chile to be
redirected to Chinese networks, potentially blocking websites such as Facebook and YouTube, which are banned in that country.

The snafu underscores the fragility of the Border Gateway Protocol, which is used to route traffic over the internet. The core net underpinning remains susceptible to man-in-the-middle attacks that can divert traffic to impostor networks.

At the 2008 Defcon hacker conference in Las Vegas, researchers demonstrated a BGP attack that allowed them to redirect traffic bound for the conference network (http://www.theregister.co.uk/2008/08/27/bgp_exploit_revealed/) to a system they controlled in New York. Also in 2008, large chunks of the internet lost access to YouTube (http://www.theregister.co.uk/2008/02/25/pakistan_blocks_youtuber/) when BGP tables inside Pakistan spread to other countries.

It's unclear how widely felt Thursday's incident was outside of Asia, IDG said. Routers frequently subscribe to several BGP routes and follow the shortest path. That means networks physically located in the US, Europe and elsewhere may have ignored the tables that traveled through China.

Related stories
Comcast (finally) brings security extensions to DNS (24 February 2010) http://www.theregister.co.uk/2010/02/24/comcast_dnssec/
At long last, internet's root zone to be secured (4 June 2009) http://www.theregister.co.uk/2009/06/04/dnssec_coming/
Turks hijack Kiwi MSN via DNS cracks (22 April 2009) http://www.theregister.co.uk/2009/04/22/msn_hijacking/
Hacking internet backbones - it's easier than you think (16 April 2009) http://www.theregister.co.uk/2009/04/16/internet_backbone_hacking/