World Socialist Web Site wsws.org

Chinese Internet shutdown linked to right-wing groups, US shell corporations

Kevin Reed
28 January 2014

Last Tuesday, the Internet in China was rendered virtually inoperable for eight hours. According to news reports, nearly all of China's Internet users—600 million people—were unable to access web sites including the popular search engine Baidu and the social media site Sina Weibo.

At approximately 3:00 p.m. Beijing time on January 21, the domain name root servers in China began rerouting all Internet traffic within the country to the web servers of two Internet companies in the US, Sophidea and Dynamic Internet Technology (DIT). Web monitoring experts also said that .com, .net and .org Internet addresses failed to load in Chinese browsers during the outage.

The US media was quick to report unsubstantiated claims that the breakdown was caused by Chinese Internet censors who made a mistake and, instead of blocking access to the Sophidea and DIT web sites, accidentally redirected all of China's Internet traffic to their servers. Aside from the fact that the theory that Chinese authorities mistakenly sent the entire Internet to two IP addresses in the US is on its face implausible, no information has yet been produced to prove this claim.

It is far more likely—based on information available in news reports—that the top-level Chinese Internet servers were hacked by right-wing opponents of the Chinese government and other cyber criminals operating within the US corporate-intelligence community.

On Wednesday, Reuters reported the comments of Xiao Qiang, an adjunct professor of UC Berkeley School of Information and expert on China's Internet controls. Confirming that the breakdown emanated from within the Chinese Internet infrastructure, Qiang said, "Our investigation shows very clearly that DNS exclusion happened at servers inside of China." He added, "But how that happened or why that happened we're not sure. It's definitely not the Great Firewall's normal behavior."

The *New York Times* and *Washington Post* reported on Wednesday that the traffic from China's domain name system servers was being rerouted to web servers owned by Sophidea and DIT. Sophidea is an Internet services firm located in Cheyenne, Wyoming and specializes in rerouting Internet traffic from one web site to another to mask domain server locations. There is very little public information available about the company or the physical location of its servers. Its director is Mark Chen.

Sophidea is connected to a firm called Wyoming Corporate Services that utilizes Wyoming's lax business laws to host shell companies in a small office in downtown Cheyenne. According to a Reuters report in 2011, Wyoming Corporate Services is the registered home of thousands of companies from all over the world, including enterprises engaged in criminal and fraudulent activities.

The Reuters report documented that the businesses operating out of Wyoming Corporate Services included: a US Department of Defense contractor who was convicted in 2007 of wire fraud in connection with selling counterfeit parts to the US military; the former Ukrainian Prime Minister Pavlo Lazarenko, who is now serving an eight-year jail term in California on money-laundering and extortion charges; and Ira N. Rubin, who created 18 different firms in connection with an illegal online gambling operation and fled to Costa Rica to avoid arrest.

The other firm that received a massive stream of Chinese Internet traffic last Tuesday, Dynamic Internet Technologies, is also a software business that offers tools for accessing web sites censored by governments in China, Syria, Iran Vietnam and UAE. Among DIT's clients are Voice of America, Radio Free Asia, Human Rights of China and *Epoch Times* (a right-wing Chinese publication affiliated to Falun Gong).

One source of the theory that the breakdown was caused by Chinese censors was an email message from Bill Xia, a Falun Gong supporter and the man who founded DIT after immigrating to the United States in the 1990s. Xia wrote that the shutdown could have been caused by a "misconfiguration" in the Chinese firewall.

"Only the Great Firewall has this capability ready," Xia wrote. Other US technology experts and media spokespeople then backed up Xia's claim, saying government censorship of the web was bound to "backfire."

A similar shutdown of the Internet in China occurred in April 2012 when web browsers were unable to access both Chinese and foreign web sites. That outage, which was never fully explained, also impacted users in Hong Kong and Japan. And last August a denial-of-service attack caused large portions of the Chinese Internet to go in what was undoubtedly a hacking operation.

While speculation continues as to the specific cause of last Tuesday's shutdown, it is not out of the question that the outage was the result of a sophisticated malware operation sponsored by the US government or one of its private contractors. As revealed by Edward Snowden in November, the NSA and its Office of Tailored Access Operations (TAO) are the number one purveyor of cyber crime and distributor of malware in the world. These operations rely upon IP address switching and domain name server tricks to lure users into unknowingly loading harmful software onto their systems.

In June, intelligence expert Matthew Aid reported that the NSA and TAO have been engaged for 15 years in a large-scale hacking operation aimed at Chinese computer and telecommunications networks.

The background and activities of DIT are of particular interest in this regard. The Wikipedia entry on DIT's flagship product, called Freegate—software that uses proxy servers to bypass Internet firewalls—contains information regarding the close association of DIT with US government agencies and NGOs since it was founded in 2001. Freegate was developed with financing from the Broadcasting Board of Governors, the government agency responsible for US imperialist propaganda through broadcasting services such Voice of America and Radio and Television Marti.

The primary function of DIT has been the penetration of China's Great Firewall, and there is evidence that Freegate has built-in capabilities for that purpose. In 2004, the anti-virus and security firm Symantec identified Freegate as a "Trojan horse," i.e., malware that is non-self-replicating and, when executed, causes data loss, theft or system harm. Shortly thereafter Symantec publicly dropped the designation, stating that it had "mislabeled" the software. In 2013, Freegate was reported as a pro-Syrian government tool of cyber warfare designed to steal information from user's computer instead of circumventing government censorship.