

China internet breakdown blamed on web address hijack tools

January 23 2014



Two Chinese men use their laptop computers at a cafe in Beijing on November 2, 2012

A firm specializing in censorship-evading technology on Wednesday blamed a massive breakdown of China's internet on website address "hijacking" tools used by authorities there.

"In 2002, China started to use DNS hijacking technology to block web

sites," said US-based Dynamic Internet Technology, which runs a tool called FreeGate designed to bypass Chinese Internet censors.

"On January 21, 2014, there was a large-scale internet breakdown in China caused by this DNS hijacking system."

Internet users were sent to an IP address operated by Dynamic Internet Technology, which runs FreeGate. The website was registered to a shell company at an address in Wyoming, according to DIT.

The IP address—65.49.2.178—is linked to dongtaiwang.com, a news portal run by Falun Gong members, Greatfire.org said.

Falun Gong is a Buddhist-inspired religious group that was banned in China in 1999 and branded an "evil cult."

Dynamic Internet Technology lists as clients on its website the Epoch Times—a publication linked to the spiritual movement—along with Human Rights in China and other groups.

Cyber-monitoring group Greatfire.org blamed China censors for the fiasco, and DIT backed that contention in a release posted at its website.

The domain name system, or DNS, is essentially an addressing method that lets computers know where to go to find websites on the Internet.

DNS hijacking happens when someone, say, a censor, intercepts transmissions between computers and sends back a wrong address directing an Internet user away from banned online destinations.

"This kind of attack requires that the attacker be able to monitor all traffic of targeted users and needs the CPU resources to process all the data," DIT said.

Web users in the country—which tightly restricts internet access—had trouble accessing numerous sites on Tuesday, said Greatfire.org, which tracks the vast Chinese online censorship apparatus known as the Great Firewall.

"We have conclusive evidence that this outage was caused by the Great Firewall," it said on its website, calling the incident "one of the largest Internet outages ever in China".

The state news agency Xinhua raised the possibility of hacking, and the official China Internet Network Information Centre attributed the breakdown to a "root server for top-level domain names".

But Greatfire.org cast doubt on those claims, citing technical tests and saying such an act was "not enough to cause this outage." China has about a half billion [internet users](#).

China's vast censorship apparatus proactively suppresses any information or websites online deemed sensitive, from popular sites such as Facebook and Twitter to a frequently updated list of search terms.

© 2014 AFP

Citation: China internet breakdown blamed on web address hijack tools (2014, January 23) retrieved 13 March 2024 from <https://phys.org/news/2014-01-china-internet-breakdown-blamed-web.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--