

Beijing behind Internet security violation: group

March 25 2015



China's cyberspace administration is 'complicit' in attacks on major Internet companies including Google, according to GreatFire.org, an anti-censorship group

China's cyberspace administration is "complicit" in attacks on major Internet companies including Google, an anti-censorship group said Wednesday, calling on firms worldwide to strengthen their defences.

Beijing dismissed the accusation and called for all sides to "abandon accusing each other without proof".

GreatFire.org, which operates websites seeking to circumvent China's vast censorship apparatus, pointed to statements by Google, Microsoft and Mozilla as showing the Chinese government was involved in so-called "man-in-the-middle" operations.

Such attacks involve an unauthorised intermediary inserting themselves between computer users and their online destinations, usually undetected, allowing them to harvest data traffic including passwords.

GreatFire.org said the firms' statements amounted to "concrete evidence" the Cyberspace Administration of China (CAC)—the government's Internet authority—and the China Internet Network Information Centre (CNNIC)—the administrator—were "behind these malicious actions and are endangering safety and security on the Internet for everyone".

The ruling Communist Party maintains tight controls over the Internet, blocking websites it deems politically sensitive in a system dubbed the "Great Firewall of China" and obliging social media companies to censor user-generated content.



Activists demonstrate for freedom of speech in China, during the CeBIT technology fair in Hanover, central Germany, on March 16, 2015

At the same time, Washington and Beijing regularly trade accusations of hacking, with FBI director James Comey declaring last October that China was at the "top of the list" of countries launching cyberattacks on US firms.

Beijing has also drawn criticism for a recent draft law that would require foreign companies to hand over their encryption keys and other sensitive data in order to do business in China.

A Google security engineer, in a posting on the company's online security blog Monday, said CNNIC and a firm called MCS Holdings had been found to have issued "unauthorised digital certificates for several Google domains".

"The misissued certificates would be trusted by almost all browsers and operating systems," he wrote, describing the resulting vulnerability as a "serious breach" of the Internet certificate authority system.

On Tuesday Microsoft and Mozilla, owner of the popular Firefox web browser, announced that they were revoking trust in all MCS certificates.

GreatFire.org welcomed the companies' response but added: "We once again call for Google, Mozilla, Microsoft and Apple to revoke trust for CNNIC immediately in order to protect Chinese user data and user data worldwide."

Asked about the accusations Wednesday, foreign ministry spokeswoman Hua Chunying said: "I think that all parties should abandon accusing each other without proof. What they should do is to press ahead with talks on forming cyber rules and to maintain cybersecurity."

Beijing frequently describes itself as a victim of hacking.

CAC and CNNIC did not immediately respond to requests for comment by AFP.

Last week GreatFire.org said it had been hit by a barrage of automated requests known as a distributed denial of service attack in an attempt to bring down its anti-censorship services.

"We are under attack and we need help," it said in a blog post at the time.

© 2015 AFP

Citation: Beijing behind Internet security violation: group (2015, March 25) retrieved 15 May 2024 from <https://phys.org/news/2015-03-beijing-internet-violation-anti-censorship-group.html>

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.