Technology Review
PUBLISHED BY MIT

Thursday, October 15, 2009

China Strikes at Internet Freedom Tool

A leading anonymity technology is targeted by the Chinese government for the first time.

By David Talbot

For the first time, the Chinese government has attacked one of the best, most secure tools for surfing the Internet anonymously. The clampdown against the tool, called Tor (http://www.torproject.org/) , came in the days leading up to the 60th anniversary of China's "national day" on October 1. It is part of a growing trend in which repressive nations orchestrate massive clampdowns during politically sensitive periods, in addition to trying to maintain Internet firewalls year-round.

"It was the first time the Chinese government has ever even included Tor in any sort of censorship circumvention effort," says Andrew Lewman, the executive director of Tor Project, the nonprofit that maintains the Tor software and network. "They were so worried about October 1, they went to anything that could possibly circumvent their firewall and blocked it."

Tor is one of several systems (http://www.technologyreview.com/computing/22427) that route data through intermediate computers called proxies, thereby circumventing government filters. To anyone watching Internet connections, the traffic then seems to be coming from the proxies. Tor provides stronger anonymity protection than most others, because it uses several such proxies and encrypts the Internet protocol (IP) addresses at each step. The downside is that Tor slows down Internet access considerably.

The potential for Tor's IP address to be blocked has always existed, especially since Tor Project publishes them openly in an online directory. Until late September, however, China never bothered to block it. Then, on September 25, Tor usage by Chinese citizens plunged from thousands of users (between 8,000 and 10,000 Tor requests from China were active at any given moment in the preceding days) to near zero. "Based on what we tested, it appears that they pulled the list on September 18, and it took until September 25 to get that into their firewall apparatus," says Lewman. On Tuesday, Tor Project published an analysis (https://blog.torproject.org/blog/picturing-tor-censorship-in-china) of China's effort.

The analysis found some good news. The use of workarounds called "bridges"--IP addresses of volunteer computers who have agreed to connect users to the otherwise-blocked Tor network--soared during the period, helping many Tor users back online. The distribution of these bridge addresses was coordinated through various instant-messaging services in China. While hard numbers were not available, Lewman says bridge use increased 70-fold.

The events of late September showed that China is stepping up its blocking efforts, said Wendy Seltzer (http://wendy.seltzer.org/) , a law professor and research fellow at the University of Colorado who founded and developed the Chilling Effects Clearinghouse (http://www.chillingeffects.org/) , a project to fight unjustified legal threats to the Internet. "Watching China step up blocking around nationally significant events shows the degree of control they are trying to exercise," added Seltzer, who is also an uncompensated member of Tor's board. "The experience helped to validate Tor's strategy of having lots of defenses in queue."

Tor is now working out ways to more efficiently and rapidly disseminate bridge addresses in the future, including via Twitter. "The issue is, obviously, that the Chinese government could also use Twitter to receive the bridges, and block those, too," adds Lewman. He is working on ways to time responses to such requests to make things more difficult for the government to block. "Writing the code is the easy part. The logic behind it--that's the hard part."

In 2006, the OpenNet Initiative (http://opennet.net/) --a research collaboration among several universities--reported filtering in 25 of 46 nations tested. In another forthcoming study, the OpenNet Initiative will report that these efforts are expanding, says Ronald Deibert, a political scientist and director of the Citizen Lab (http://www.citizenlab.org/) at the University of Toronto, one of the participating universities.

The trend of time-sensitive national crackdowns has increased in the past four years, Deibert says. "Often governments block access to information not as static or passive filtering walls, but rather at key moments in time when the information has most value, such as during public demonstrations, key historical events, or election periods," notably including, in recent months, the disputed Iranian election, he adds.