Roar of China's 'Great Cannon' heard across the internet

April 15 2015, by Tim Stevens

Big guns for big jobs. Credit: archer10, CC BY-SA

China has once again surprised researchers by unleashing what has been dubbed its "Great Cannon" – a cyber weapon that has in recent weeks brought down several websites including the Github software code repository and GreatFire, an activist group working against censorship in China.

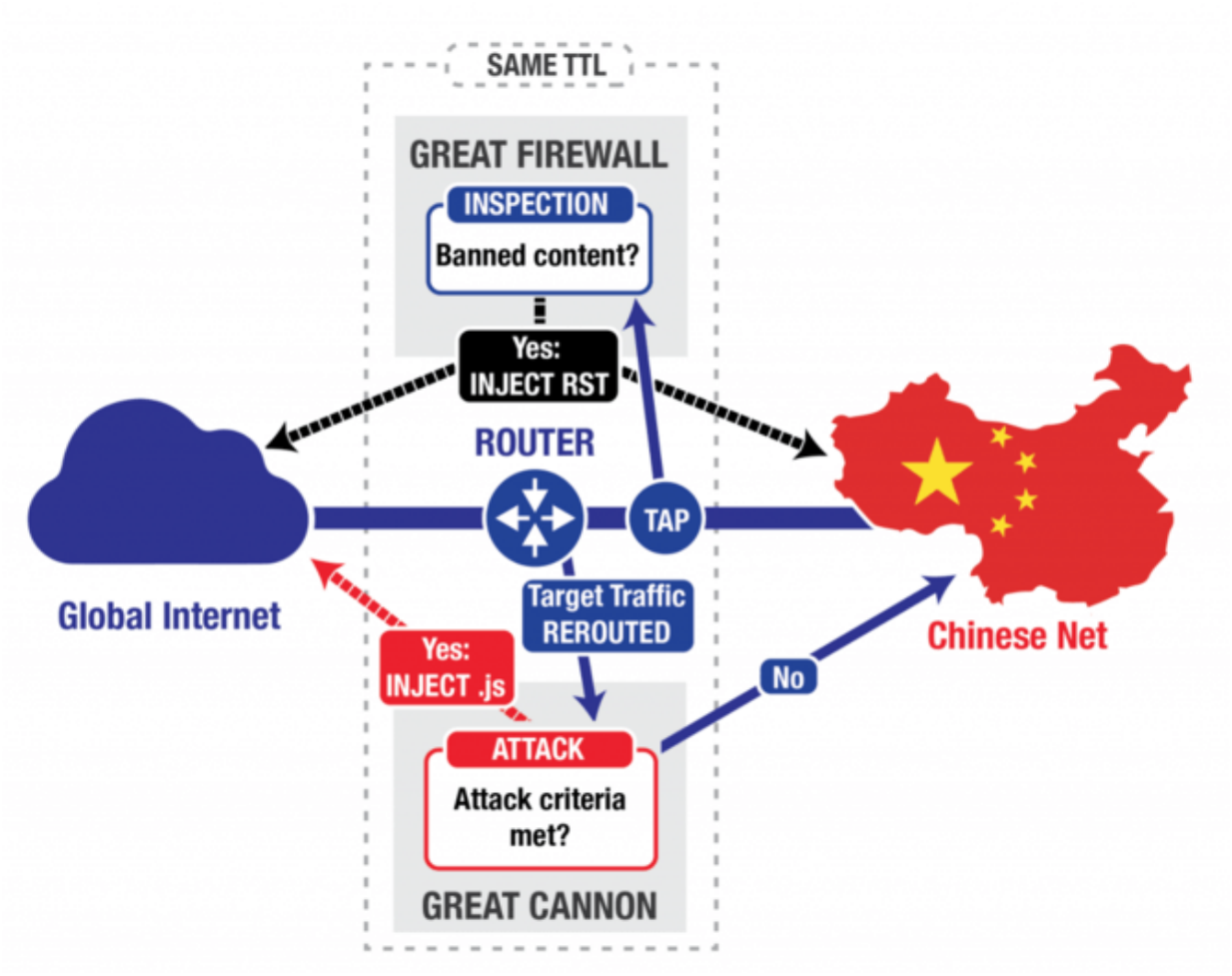
The offensive power of the cannon is closely linked to the defensive nature of the so-called Great Firewall of China, an internet control system that prevents citizens from accessing websites banned by the ruling party.

Researchers at the University of Toronto's Citizen Lab have released a detailed analysis of the attacks against GitHub and GreatFire. While the firewall works by intercepting traffic destined to or from banned websites, the cannon works by intercepting huge amounts of unencrypted web traffic passing through Chinese-controlled networks and re-routing it to a specific target. Such a deluge of traffic becomes a distributed denial of service (DDoS) attack, a tried-and-tested method in which the scale of requests overwhelms the site's web servers, essentially knocking it offline.

Who's pointing the cannon?

The identities of the Great Cannon's targets provide circumstantial evidence of the Chinese government's involvement. GreatFire provides real-time information on the status of Chinese internet censorship, allowing Chinese web users the possibility of avoiding keywords banned by the censor, and finding other ways around the Great Firewall. GreatFire also hosts two GitHub software repositories, one of tools for circumventing China's Great Firewall, the other a mirror for The New York Times – hardly a Communist Party favourite.

That either might be a suitable target for the Chinese government is readily apparent, but the Citizen Lab researchers also found firmer evidence that the cannon is indeed of Chinese government origin. The Great Cannon and Great Firewall share a number of technical similarities that suggest a common origin. And they are located within the same network address space – somewhere within both the state-run firms of China Telecom and China Unicom.



How the Great Firewall and Great Cannon are linked. Credit: Citizen Lab

If these forensic conclusions are correct, why would the Chinese government not hide both the existence and use of this capability better, particularly given that attacks of this nature flout international norms and are illegal in most jurisdictions?

Sabre-rattling on the world stage

The first possibility is that these attacks serve a short-term objective of countering the actions of entities China considers threats to its national security. This is a long list, that includes virtual private network and proxy providers, various non-governmental organisations and the Western media.

GreatFire for example has been significantly affected by the attack and its ability to conduct what it calls "collateral freedom" is greatly diminished. This might be considered a success by elements of the Chinese state apparatus, although any tactical gains are likely to be short-lived. Perhaps showing its hand so early in the game will make its Great Cannon less useful in the future, as other organisations are alerted to its characteristics.

At the same time, that the Chinese are prepared to weaponise the traffic passing through their networks into forming the Great Cannon demonstrates both the state's capability and its willingness to deploy that capability. These are essential components in any attempt to deter opponents, state or non-state, who might attempt to degrade or circumvent Chinese state censorship. "Firing" the cannon may be an attempt to establish it as a credible deterrent – GreatFire's web hosting costs rocketed to US$30,000 per day due to the explosion of traffic.

The Citizen Lab researchers also note that the Great Cannon can be used to deliver other payloads, more malicious ways of targeting and compromising foreign internet addresses than the relatively crude DDoS attacks launched in March. This must concern other states, although we do not know how it might affect their actions.

Casting a pall over international relations

Someone or, more likely, some committee, within the party apparatus may have made a strategic decision that the benefits of demonstrating

this capability outweigh the costs of attracting international condemnation for doing so. The only response the Chinese government has offered is its well-worn line that China is itself a target of foreign computer attacks – which while true hardly deflects criticism or allays suspicion.

China knows well that the US National Security Agency and UK GCHQ have already been found guilty of interfering with foreign networks but an appeal to this precedent no more exonerates China than it would any other country.

China and the US, its peer-competitor, have been trading blows in this fashion for many years. Far from dampening this mutual distrust, these latest actions only serve to heighten it. Given the global importance of China-US relations, this is not a development to be welcomed.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation

Citation: Roar of China's 'Great Cannon' heard across the internet (2015, April 15) retrieved 3 May 2024 from https://phys.org/news/2015-04-roar-china-great-cannon-heard.html