Massive denial-of-service attack on GitHub tied to Chinese government

By Dan Goodin

Published: 2015-03-31 · Archived: 2026-04-06 00:46:03 UTC

"This attack demonstrates how the vast passive and active network filtering infrastructure in China, known as the Great Firewall of China or 'GFW,' can be used in order to perform powerful DDoS attacks," the Netresec researchers wrote in a [report published Tuesday](). "Hence, the GFW cannot be considered just a technology for inspecting and censoring the Internet traffic of Chinese citizens, but also a platform for conducting DDoS attacks against targets world wide with help of innocent users visiting Chinese websites."

The report included the following data, which was taken using the tshark packet sniffer. It shows that the TTL of a legitimate SYN+ACK packet is 42, while three packets with a malicious payload have TTL values of 227, 228, and 229. The results suggest that the SYN+ACK packets are coming from the actual Baidu server, while the packets carrying the malicious payload are injected somewhere else:

> tshark -r baidu-high-ttl.pcap -T fields -e ip.src -e ip.dst -e tcp.flags -e ip.ttl
> 192.168.70.160 61.135.185.140 0x0002 64 <- SYN (client)
> 61.135.185.140 192.168.70.160 0x0012 42 <- SYN+ACK (server)
> 192.168.70.160 61.135.185.140 0x0010 64 <- ACK (client)
> 192.168.70.160 61.135.185.140 0x0018 64 <- HTTP GET (client)
> 61.135.185.140 192.168.70.160 0x0018 227 <- Injected packet 1 (injector)
> 192.168.70.160 61.135.185.140 0x0010 64
> 61.135.185.140 192.168.70.160 0x0018 228 <- Injected packet 2 (injector)
> 61.135.185.140 192.168.70.160 0x0019 229 <- Injected packet 3 (injector)
> 192.168.70.160 61.135.185.140 0x0010 64
> 192.168.70.160 61.135.185.140 0x0011 64

Researchers from GreatFire have issued [their own report]() that also lays out evidence the attacks could not have been carried out without the cooperation of Chinese authorities. In an [accompanying blog post](), they went on to name the Cyberspace Administration of China and its head Lu Wei. The GreatFire researchers wrote:

> Inserting malicious code in this manner can only be done via the Chinese Internet backbone. Even if CAC did not launch the DDoS attack directly, they are responsible for managing the internet in China and it is not possible that they did not know what was happening. These attacks have occurred under CAC's watch and would have needed the approval of Lu Wei.
>
> Lu Wei and the Cyberspace Administration of China have clearly escalated the tactics that they use to control information. The Great Firewall has switched from being a passive, inbound filter to being an active and aggressive outbound one. This is a frightening development and the implications of this action extend beyond control of information on the internet. In one quick movement, the authorities

> have shifted from enforcing strict censorship in China to enforcing Chinese censorship on internet users worldwide. CAC can launch these attacks quickly and easily and they have the technical and financial resources behind them to continue to launch DDoS attacks against any website, anywhere in the world.
>
> These attacks also illustrate the shortsighted nature of the Chinese authorities. Weaponizing Chinese internet services stifles global confidence in Chinese entrepreneurs and contributes to the fragmentation of the global internet. The SEC has already asked Weibo to explain how the censorship apparatus works – Baidu, a publicly-listed company in the US, may be called in to do the same.
>
> We correctly predicted last year that China would increase their use of MITM attacks in an effort to censor encrypted websites. We now sadly predict that the DDoS attacks against us and GitHub are likely to signal a ramping up of attacks against foreign internet properties. These kinds of attacks should draw scorn and criticism from government officials of all countries around the world.

So far, there are no reports of Chinese officials responding to the accusations. In fairness, readers should remember that assigning responsibility to Internet-based attacks is extremely difficult. Attackers often manipulate their hacks to give the appearance they originated somewhere else. Still, there’s no doubt that Chinese authorities carefully police that country’s Internet backbone. It’s hard to imagine how malicious code could be inserted into so many different China-based websites for five days straight without a government authority actively participating, or at least looking the other way, while it happened.

Source: https://arstechnica.com/information-technology/2015/03/massive-denial-of-service-attack-on-github-tied-to-chinese-government/