China has at least 10 PoP presence points to hijack the network architecture

China is using BGP hijack and creating new paths for network traffic in Western countries through one of their largest telecommunications companies.

China is using BGP hijack and creating new paths for network traffic in Western countries through one of their largest telecommunications companies. At the very least, these attacks have begun since they signed with the US a ceasefire agreement for cybercrime. Points of discovery are located in the US and Canada.

According to a study by the US Naval University and Tel Aviv University, China has hijacked the backbone of Western countries' Internet since 2015. This study was published in the scientific journal Military Cyber ?? Affairs.

Chine Telecom, one of the leading telephone and network companies in China, has exploited PoP (points-of-presence) presence to implement a man-in-the-middle intervention. . CNET explains that PoP is merely a data center that directs traffic between small networks to make the Internet.

Internet traffic travels through automated systems (AS - autonomous systems) through the BGP protocol (border gateway protocol). But BGP does not have security features, so interfering with data is not difficult. This is called BGP hijack and happens quite often. However, in most cases, hijack often happens for misconfiguration, not intentionally causing poisoning, so it will be fixed in a few minutes to a few hours.

According to researchers, China has deliberately used China Telecom to implement BGP hijack. They began working in 2015, shortly after signing an agreement with the US under President Obama that will stop support for cybercriminals stealing intellectual property. 'This is a new way to get information while still complying with the agreement', in the written study 'because the agreement is only valid for military operations'.

CTG IP points in the US and Canada

The study monitored BGP abuse by building a BGP monitoring and surveillance system. Thereby, they can identify similar behavioral patterns that may want to implement intentional hijack. They found 10 PoP points used to attack - 8 points in the US and 2 points in Canada. These points were silently built from the early 2000s.

'Using these PoP points, [China Telecom] hijacked network traffic in the US and switched to China for days, weeks and months'. 'Although it can be explained by normal BGP behavior, this type of attack is intentionally harmful, precisely because of the abnormal conversion, such as making the path of longer traffic or an unusual period of time.

'Easy navigation, copying data by controlling important transit points on a nation's network architecture is a response that needs to respond quickly'.

See more:

1. Things to know when buying Chinese technology items
2. US intelligence recommends against using Huawei and ZTE phones
3. China banned VPN services to build the Great Wall