

22 May 2009

By: Lucian Constantin, Web News Editor



DDoS attack causes massive Internet blackout in China  
InfoServe365

## [DDoS Attack Leaves Five Chinese Provinces Without Internet](#)

### *Unexpected DNS chain reaction responsible*

Millions of Chinese Internet users from the Shanxi, Guangxi, Zhejiang, Jiangsu and Hebei provinces had trouble getting online on Tuesday, because of a domain name system (DNS) chain reaction caused by an initial denial of service attack against a single provider.

DNSPod, a Chinese DNS provider and domain registrar, was targeted by unknown parties, who launched a Distributed Denial of Service (DDoS) attack against the company's servers. Such an attack occurs when a hacker commands thousands or tens of thousands of compromised computers to flood a server with bogus data packets until all of its available resources are consumed trying to process them and the server becomes unresponsive to everyone using it.

Fending off attacks of this type is no easy task, even for large companies with an expensive infrastructure. Because it is nearly impossible to filter the packets received from the offending IP addresses, due to their sheer number, Internet Service Providers have automated mechanisms in place to cut all traffic towards the target.

This is what happened during the DNSPod incident, however, it triggered a chain of unexpected events, which led to network congestions for the carrier networks. DNSPod's servers happen to be used by Baofeng, a highly popular Chinese video streaming service. Once the millions Baofeng users fired up their desktop application, all the requests bounced off on the ISP servers, which did not know how to process them.

The intense traffic on the high-level servers caused bottlenecks, slowing everyone's Internet connection down to a crawl. In addition to the users in the five aforementioned provinces, who were severely affected, customers in Henan, Anhui and Gansu have also [reportedly](#) experienced problems.

Following the DDoS, which is also said to have influenced the accessibility of Baidu, China's number one search engine, the Ministry of Industry and Information Technology has issued a statement saying that, "Carriers and related firms should do more back-up to avoid similar incidents."

Other IT professionals and experts in China have also condemned the incident, arguing that fail-safe mechanisms should have been in place and that it's unacceptable for a country with over 300 million Internet users to not be able to avoid such cases. Baofeng has announced that, in three days' time, it will complete installing backups for its primary DNS servers.