Yandex suffered the largest DDoS attack in history

A constantly growing DDoS botnet has targeted Russian search engine Yandex for over a month.

Yandex is also known as "Russian Google" and at the peak they suffered an attack with a scale of up to 21.8 million access requests per second.

The new botnet is named Meris and it consists of tens of thousands of devices controlled by hackers. The researchers believe that most devices in the Meris botnet are high profile network accessories.

The Russian press described Meris' attack on Yandex as the largest in the history of the Russian internet (aka RuNet). Details of the attack have just been shared by Yandex and their anti-DDoS partner, Qrator Labs.

According to information gathered from several single attacks, the force of the Meris botnet amounted to more than 30,000 devices. Meris (M?ris) is a Latvian word meaning calamity.

From the data that Yandex tracks, the attack on their server was conducted based on about 56,000 clues. However, researchers have discovered indications that the number of devices that the people behind Merit are controlling may be closer to 250,000.

The difference between the number of devices used to attack and the number of devices being controlled showed that Meris had not yet used its full power. Besides, the Meris botnet is not made up of weak IoT devices but powerful network devices with Ethernet connectivity.

Meris is by far the highest-traffic attack-generating botnet that Cloudflare has recorded and prevented. That attack peaked at 17.2 million requests per second (RPS).

However, that record was broken by Meris herself when she attacked Yandex on September 5 with a traffic of 21.8 million RPS. Yandex has suffered several attacks in the past month with increasing intensity:

1. August 07: 5.2 million RPS
2. August 9th: 6.5 million RPS
3. August 29: 9.6 million RPS
4. August 31: 10.9 million RPS
5. September 5th: 21.8 million RPS

According to the researchers, to deploy an attack, Meris relies on a SOCKS4 proxy on hacked devices, using DDoS techniques over HTTP connections and port 5678. Meanwhile, the devices that Meris controls are all devices. is related to MikroTik, a Latvian manufacturer of networking equipment with mainly corporate clients.

Most devices controlled by Meris have ports 2000 and 5678 open. In which, MikroTik uses public 5678 for the MikroTik Neighbor Discovery Protocol (MikroTik Neighbor Discovery Protocol).

When searching the public internet, researchers discovered 328,000 servers with open TCP port 5678. However, not all of these were MikroTik devices. Currently MikroTik has been informed about this issue.