Brief technical analysis of the "Gorilla" botnet

By Federal Department of Defence, Civil Protection and Sport DDPS

Archived: 2026-04-02 10:38:55 UTC

Brief technical analysis of the "Gorilla" botnet

10.10.2024 - In September 2024, the NCSC recorded an increase in DDoS attacks carried out by a botnet called "Gorilla". This is a "DDoS-as-a-service" service offered on Telegram, which can be rented for some fee. As an operator of a critical infrastructure in Switzerland was affected by such DDoS attacks, the NCSC has published the technical findings in a short report.

Last September, the NCSC received a report from a national critical infrastructure operator about an overload attack (a so-called "DDoS" attack) against its infrastructure. The technical analysis carried out together with the critical infrastructure showed that the DDoS attack was presumably carried out by a "DDoS-as-a-service" service, which is offered on the Telegram channel under the name "Gorilla Services", among others. The NCSC was able to identify the infrastructure used by the attackers and initiate appropriate defence measures. In addition, the Telegram channel of "Gorilla Services" was shut down by means of a complaint sent to Telegram.

The technical report sheds light on the infrastructure used by the "Gorilla" botnet and the malware used by the attackers. The malware has code similarities to the "Mirai" and infects devices with a Linux/Unix operating system. The malware receives attack commands from a central botnet command & control server and executes them accordingly.

The DDoS attacks against Swiss infrastructures were DNS amplification attacks. In these attacks, extremely large data streams are directed at the victim's infrastructure by misusing the Domain Name System (DNS), thereby overloading it. While the attacks led to short interruptions of some services, the security and integrity of data was not at risk at any time.
