SEMINARS
WORKSHOPS
ACADEMY

zeroBS

Secur|Ty made in Germany

zeroBS DDoS-Training

for Admins and Operations

Graphic: Screenshot Dashboard

DDoS Stresstest

zero.bs operates a dedicated, cloud-based platform to conduct DDoS test attacks on networks, appliances and applications. With the help of this platform, we check the effectiveness of your DDoS defense mechanisms.

OUR WORK

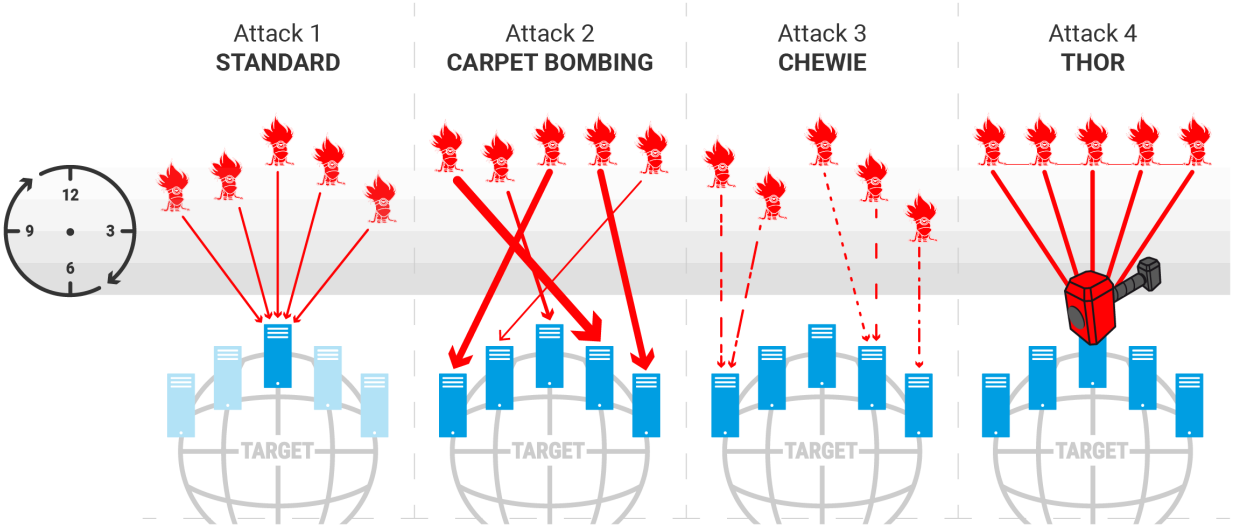
In addition to team training and reviewing the anti-DDoS measures, more and more the performance of performance records is the focus of our stress tests. We have extensive experience in testing the entire chain, from BGP-side entypoint to anti-DDoS appliances, firewalls, load balancers and application servers.

SUCCESSFULLY TESTED

Below you will find a selection of manufacturers, technologies and providers we have already analyzed.

Part of our stresstest are comprehensive analyzes (OSINT) in advance and integrated monitoring of attacked targets in order to be able to make qualitative, measurable statements on performance and limits.

ATTACKMODES



- **STANDARD:**
  Single-IP-Attacks, perfect for basic certificates of performance
- **CARPET BOMBING:**
  Attacks against whole Networks/CIDR-Ranges, necessary for advanced tests and increased threatlevels
- **CHEWIE-ATTACK** (CarpetBombing v 2.0):
  even more randomness, to tangle any statistic-based detection
- **THORS HAMMER:**
  an to the exact millisecond timed Attack (Thors Hammer), based on our own R&D with devastating success.

FEATURES

- volumetric attacks up to 100 GB/s or 100 Mio pps, TCP, UDP or ICMP
- Layer-7-Attacks with full-stack-browsers, up to 10 Mio RPS
- 50 locations and up to 100.000 dedicated IPs available
- full automated setup and orchestration
- dashboard and monitoring for clients
- monitoring-logfile and export for further analysis
- simulation of real-world-botnets (server, IoT, Mirai etc)
- customizable attacks, if necessary
- interactive dashboard: every attack is recorded and can be replayed for later analysis
- multi-location-monitoring

REASONS FOR A STRESS TEST

- performance record for the individual network components
- check whether DDoS protection measures work as desired (proof of function),
- Measuring your own protection level compared to the threat level according to the DDoS Resiliency Score
- Test if administrators are adequately trained for a DDoS attack
- Optimize the workflow in the event of a DDoS attack
- Estimate the effects of a successful attack
- Estimate the cost / effort of a successful attack

THE FOLLOWING TARGETS/TECHNOLOGIES CAN BE TESTED

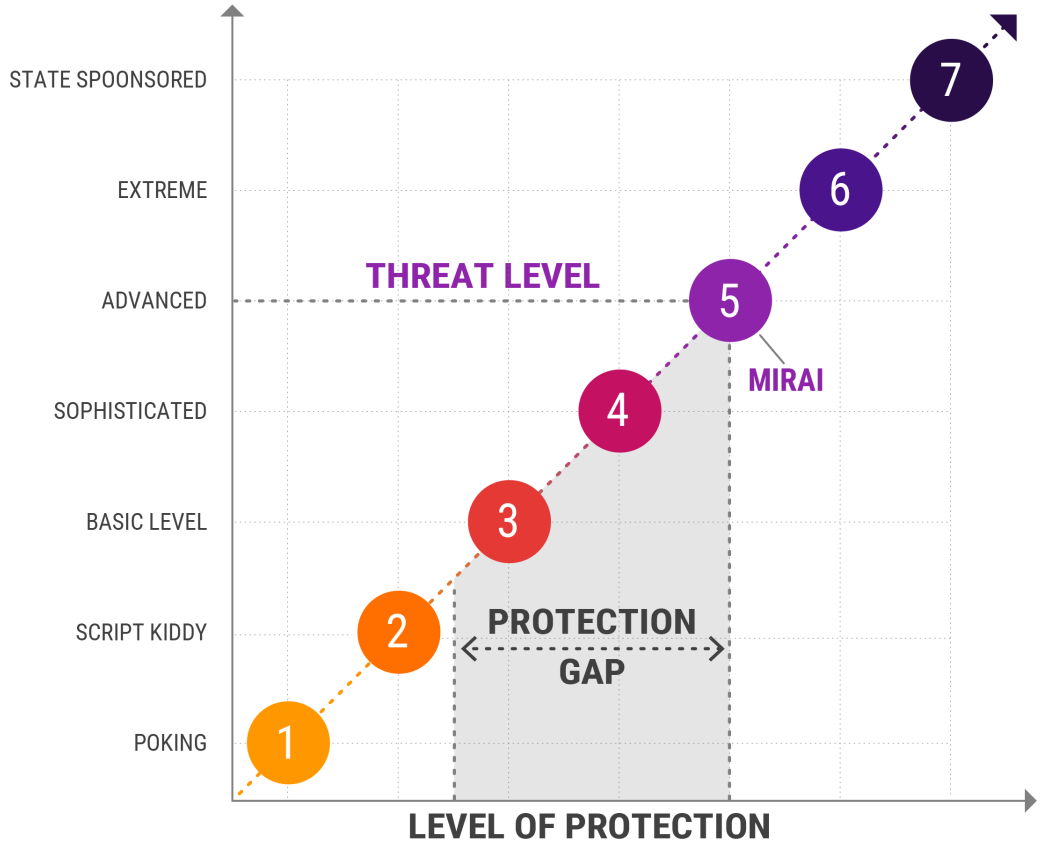
- networks
- BGP routers
- Firewalls and VPN gateways
- Web server / Web infrastructure
- APIs
- SSL-Offloader
- Loadbalancer
- DNS Infrastructure
- any TCP services
- DDoS-Appliances
- WebApplicationFirewalls
- IDS / IPS
- CDNs
- cloud-based DDoS protection (Akamai, CloudFront, CloudFlare)
- Inhouse DDoS protection

ATTACK VECTORS

- Layer 3/4 (volumetrics attacks)
- Layer 7 (attacks on applications)
- Botnet-Simulation
- Attacks against firewalls
- Attacks against load balancers
- DNS Waterboarding
- over 50 different attack types
- CDN-Reflections
- individually designed attacks
- Real World Botnet Simulations (10,000 IPs)
- Paperwork and dry run exercises to test emergency workflows

DRS – DDOS-RESILIENCY-SCORE

Our rating is based on the "DDoS Resiliency Score" (DRS) instead of and can be traced at any time and comparable.



PLATFORM – STRUCTURE / PROCESS

- **CABRIO:** Planning, provisioning of the required pods (assembly / dismantling, number and regions)
- **LOIC:** Remote control for actual attack activity during an assessment
- **DASHBOARD:** Live dashboard and monitoring for customers and reports