zeroBS

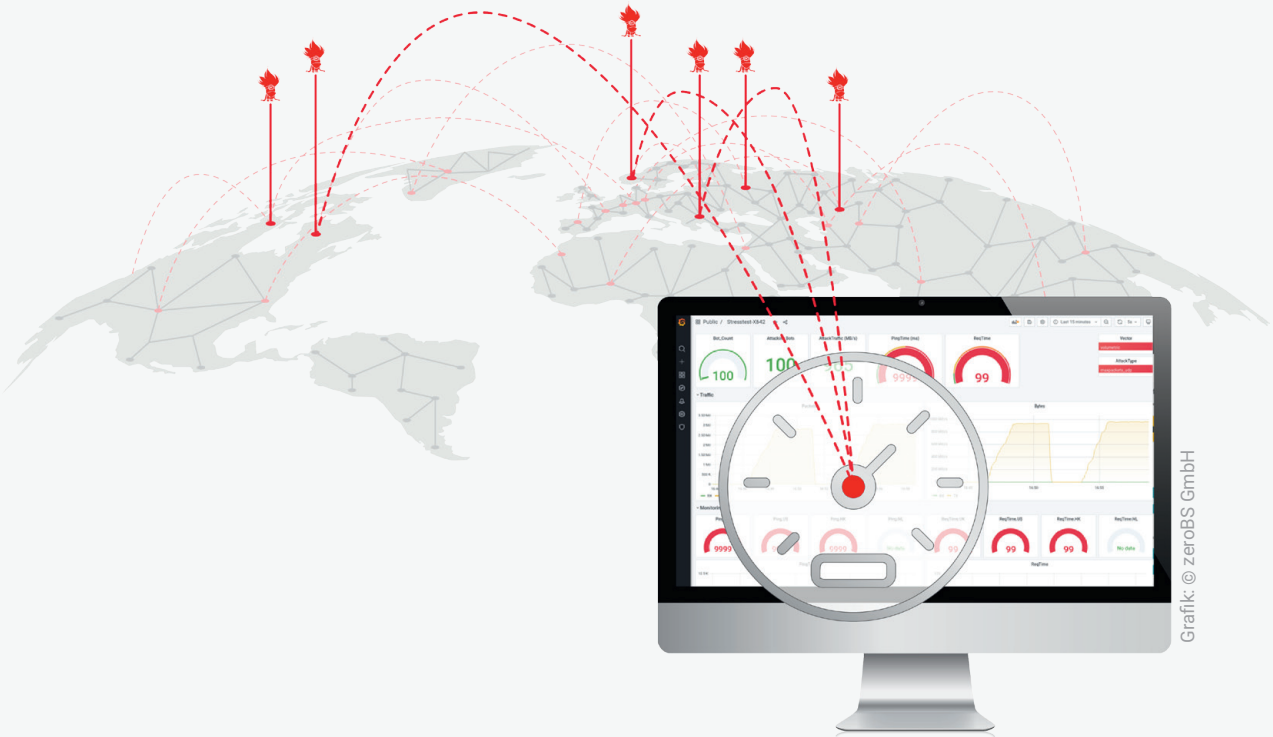
SecurITy made in Germany

zeroBS

DDoS-Stresstest

For Admins and Operations

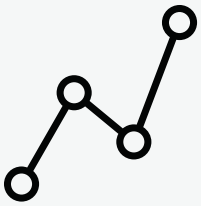
Guarantee the availability of your business operations and test your infrastructure with our state-of-the-art, cloud-based threat simulation platform.



Grafik: © zeroBS GmbH

Advances DDoS-Stresstest

Take advantage of the opportunity to not only realistically assess your existing infrastructure on the basis of individual, failure-free DDoS stress tests, but also to proactively improve it.



DDoS-TEST – Know How

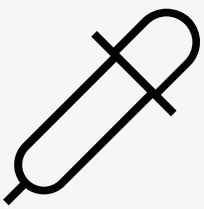
Methods for measurability, evaluation and comparability during / after a test.

THREAT-LEVEL Determination

Test own level of protection / Proof of performance and location determination.

WORKFLOW optimise

Workflow training with live monitoring under real attack conditions in real time.



ANALYSIS

Estimation of effects and costs as well as expenses in the event of a successful attack..

Introduction

zeroBS is a pioneer in the field of IT security and offers a dedicated, cloud-based platform that has been specially developed for carrying out DDoS stress tests.

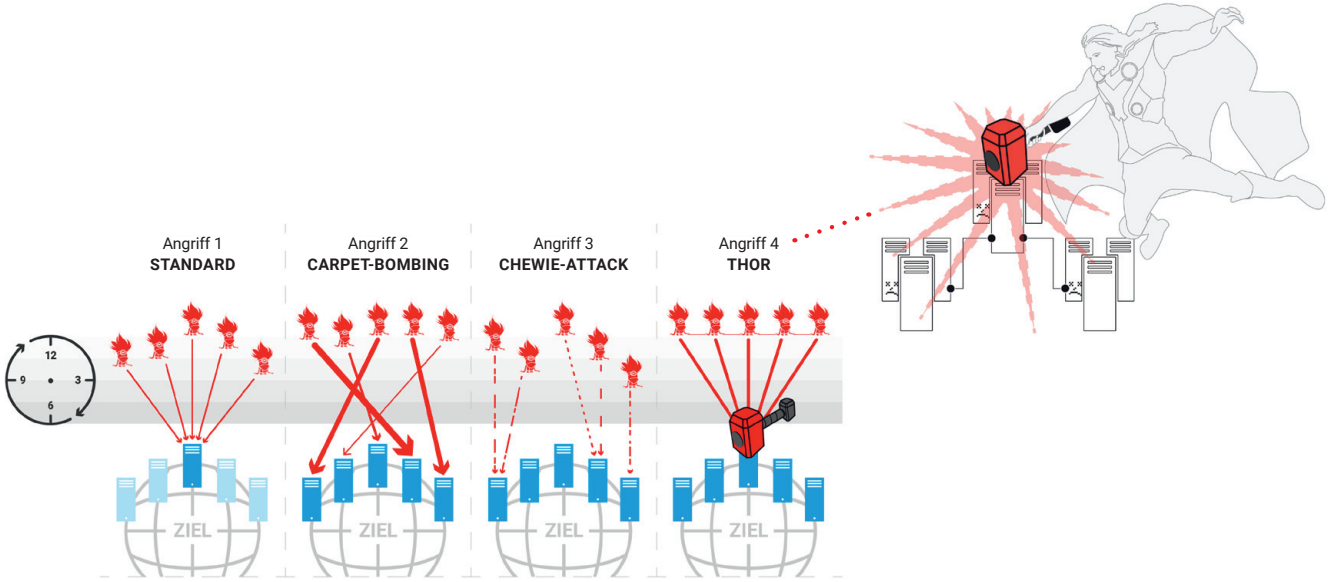
Other core competences lie in the simulation of network attacks and the testing of protection mechanisms for your infrastructure.

Our customisable platform enables targeted tests in the form of layer 3, 4 and 7 attacks and also IPv6 protocols. We evaluate the resilience of your systems from various entry points such as: existing anti-DDoS appliances, firewalls, load balancers, application servers – including BGP-side entry points. However, the importance of DDoS stress testing goes beyond purely technical aspects: it also serves as an effective method of training your team while determining the performance limits of your infrastructure.

Using comprehensive analyses in advance and integrated monitoring of attacked targets, you can gain meaningful insights into the performance of your systems.

In our networked world, protecting your infrastructure from network attacks is crucial. Our DDoS stress tests offer you the opportunity to test attack scenarios of any type and scope in real time: **take your IT security to a new level.**

Attack Modes



1 **Standard – attack on individual IPs:** ideal for proof of performance / retests

2 **CarpetBombing – Attack on entire networks:** necessary for advanced proof of performance and increased threat levels*

3 **ChewieAttack – CarpetBombing v 2.0:** each attacker IP only sends traffic for max. 30 seconds, then goes into standby and searches for a new target after 2 minutes**

4 **Thor – Attack tuned to the millisecond (Thors Hammer):** an in-house development with resounding success

***Def. CarpetBombing von APNIC Global DDoS attack trends 2018**
Carpet bombing attacks are a new variant of the more common reflection or flooding attacks, where instead of focusing the attack on a single destination, the attacker attacks every destination within a specific subnet or CIDR block (for example, a /20). This will both make it more difficult to detect the attack and also to mitigate it, potentially resulting in outages due to the flood of attack traffic across network devices and internal links.

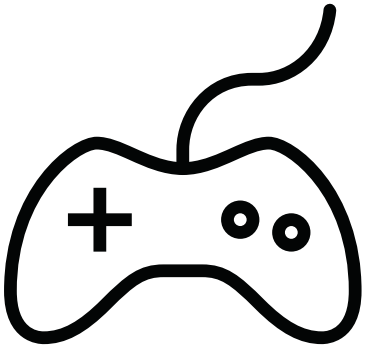
In addition, these attacks are often fragmented, resulting in a flood of non-initial IP fragments, which can be tricky to mitigate. The attacker will often shift their attacks from one subnet (or CIDR block) to another, complicating the detection and mitigation even further.

****Def. ChewieAttack (CarpetBombing 2.0)**
Very similar to Carpetbombing in terms of target selection, the Chewie attack introduces more randomness into the game by selecting target, strength, vector and protocol completely at random.

This ensures that pure statistics-based detection methods are completely confused, as the packet stream from an attack IP never lasts longer than 30 seconds, and then stops for at least 120 seconds, only to restart with a new target and pattern.

Although only 25% of the bots in a botnet are active at any one time, the attack is much more difficult to defend against.

Features



+ Volume attacks up to 100 GB/s or 100 million pps via TCP, UDP or ICMP
+ Layer 7 attacks with full-stack browsers, up to 10 million RPS
+ 50 locations, up to 100,000 IPs possible
+ IPv4 and IPv6
+ Automated setup and orchestration of the infrastructure
+ Dashboard and Monitoring
+ Exports and Logs for easy tracking and analysis
+ Simulation of real botnets (server, IoT, Mirai etc)
+ Fully customisable attacks
+ Interactive dashboard: every attack is recorded and can be replayable for later analysis
+ Multi-Location-Monitoring

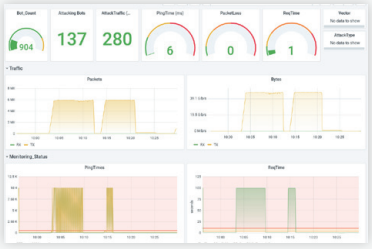
We test these targets (a.o.)

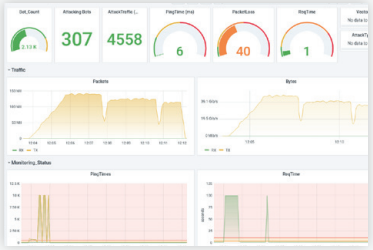
+ **Networks**
+ **BGP-Router**
+ **Firewalls and VPN-Gateways**
+ **Webserver / Web-Infrastructure**
+ **APIs**
+ **SSL Offloader**
+ **Loadbalancer**
+ **DNS-Infrastructure**
+ **any TCP-Services**
+ **DDoS-Appliances**
+ **Layer 3/4 (Volume attacks)**

Attack vectors

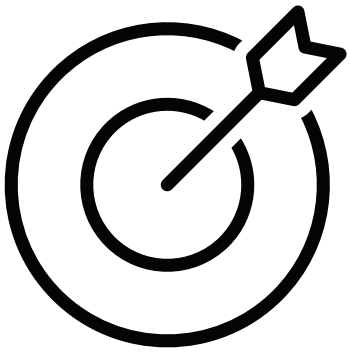
+ **Layer 7 (Application-Attack)**
+ **IPv4 or IPv6**
+ **Attacks against Firewalls**
+ **Attacks against Loadbalancer**
+ **DNS-Waterboarding**
+ **CDN-Reflections**
+ **over 50 types of attack**
+ **customised attacks**
+ **Real-World-Botnet-Simulations (10.000 IPs)**
+ **Paperworks and dry runs for emergency workflows**

Screens Dashboard





Further reasons for a stress test



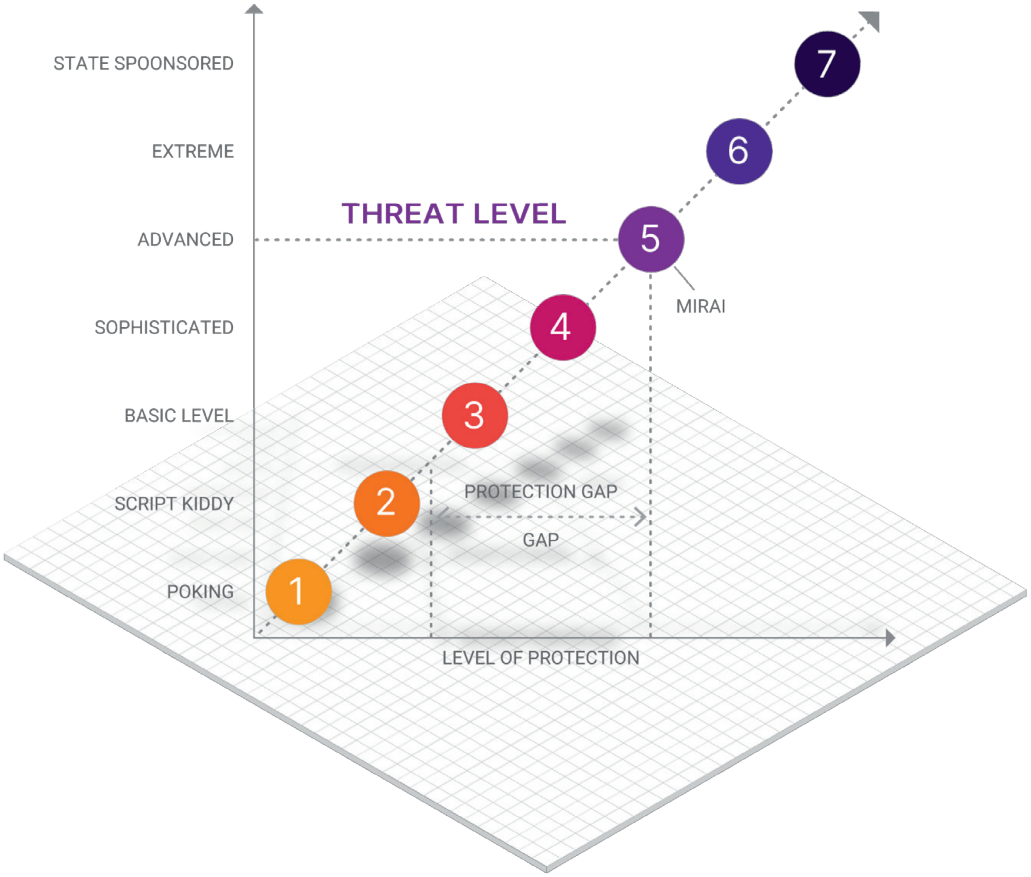
+ **Proof of performance for the individual network components**
+ **Check whether DDoS protection measures work as desired (proof of function)**
+ **Measuring your own level of protection compared to the threat situation according to DDoS Resiliency Score**
+ **Administrator test: trained and ready for a DDoS attack?**
+ **Optimising the workflow in the event of a DDoS attack**
+ **Assessing the impact of a successful attack** and
+ **Estimating the costs/expenses of a successful attack**

Benefit: Proof of performance and compliance

Our stress tests are increasingly focussing on providing proof of performance. We support companies and institutions with business-critical internet presences or specific audit requirements in the area of cyber security in the provision, implementation and organisation of all necessary proofs of performance (including reports).

DRS – DDoS-Resiliency-Score

We use the DDoS Resiliency Score (DRS) to categorise the respective level of protection in comparison to the threat situation in a way that is also comprehensible for our customers.



What makes us special

zeroBS GmbH understands both the complexity of threat environments and the challenges involved in optimising your company systems and infrastructure.
On this basis, we map attack vectors tailored directly to your needs at various levels of intensity: our expertise for your team training (redteaming) or individual tests.

References of our work

We have already successfully tested these manufacturers, technologies and providers, among others:

In addition to extensive analyses in advance, our stress test includes integrated monitoring of the targets under attack in order to be able to make qualitative, measurable statements regarding limits and performance.

Platform - Structure / Procedure

+ **Cabrio:** Planning, provisioning of the required pods (set-up/dismantling, number and regions)
+ **LOIC:** Remote control for actual attack activities during an assessment
+ **Dashboard:** Live dashboard and monitoring for customers and reports