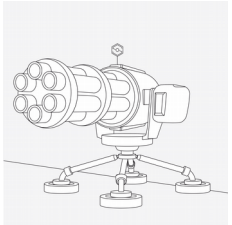
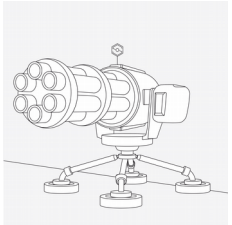
# ZeroBS // DDOS Attacker-Capabilities-Scoring



| | Botnet-Size | OldSchool | Volumetric | Layer 7 | IP-Spoofing | Recon + Monitoring | Multi-Vector | GeoIP-Region | Persistence | Costs |
|---|---|---|---|---|---|---|---|---|---|---|
| **Level 7 // GodMode** | unlimited | all | unlimited | unlimited | yes | yes | yes | yes | weeks | limitless |
| **Level 6 // Extreme** | 500.000 | all | 2 TB | > 10 Mio RPS | yes | yes | yes | yes | weeks | 5000$/day |
| **Level 5 // Advanced** | 50.000 | all | 1 TB | 10 Mio | yes | yes | yes | | days | |
| **Level 4 // Sophisticated** | 5.000 | all | 500 GB | 1 Mio | | maybe | maybe | | days | 50$/Day |
| **Level 3 // Basic** | 1.000 | some | 50 GB | 10k | | | | | hours | 50$/Month |
| **Level 2 // Skiddo** | 10 | some | 1 GB | 1k | | | | | hours | |
| **Level 1 // Poking (F5 F5 F5)** | 5 | | | 1k | | | | | minutes | |

**TLP:GREEN**

# ZeroBS // DDOS Attacker-Capabilities-Scoring



## Explanation

Capabilities for all Levels have been observed in the wild by zerobs [1] or  by third.party [2]

**Level 7 // GodMode**
- State Sponsored [2/r.3]

**Level 6 // Extreme**
- highly sophisticated individuals for rent  that can leverage month-long campaigns with precision and playing with ops-team  [1/r.1]
- teams that hit-and-run, but show no ransom, maybe just to burn a weapon for all like memcached – case
- dorian gray network (100k ddos-network that sits still since years)

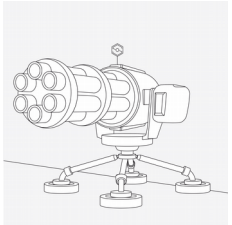
**Level 5 // Advanced**
- ddos-extortion-gangs with the capability to hit [2/r.2]
  Lazarus Bear, Armada Collective
- ddos-gangs for rent with good track-record (the better ones)

**Level 4 // Sophisticated**
- That Guy in the Basement with knowledge [1]
- DDoS-Gangs for Rent, the cheaper ones [1]
- minimum-Level for basically all ECommerce-Applications

**Level 3 // Basic**
- Booter-Networks
- Wordpress-Botnets

**Level 2 // Skiddo**
- that guy that can download a script from github

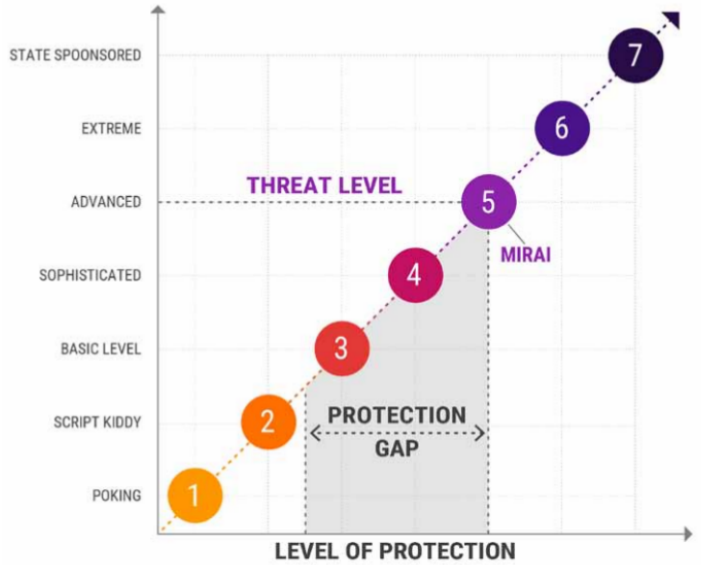
**Level 1 // Poking**
- basically F5 F5 F5

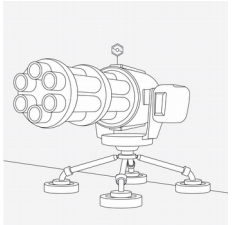


## How measuring a possible protection gap works

use an DDoS-expert for the following

- measure your threatlevel, either by industry, recent ddos-campaigns or blackmail-threat
  - banks are usually 5-6
  - ecommerce 4-5
  - smaller ISP 5-6
  - if there is an actual campaign going on against your industry, usually 5
- measure your protection – level by stresstest/assessments (preferred) or by paperwork
- if you protectionlevel doesnt meet your threatlevel, you have a protectiongap that should be adresses
- you now are able to number the costs to close the gap (good for C-level) and to calculate, if this is money spent well or not





References:


- r.1 https://zero.bs/ddos-incident-response-ein-bericht-von-der-front.html
- r.2 https://www.netscout.com/blog/asert/lazarus-bear-armada-lba-ddos-extortion-attack-campaign-october
- r.3 https://cloud.google.com/blog/products/identity-security/identifying-and-protecting-against-the-largest-ddos-attacks