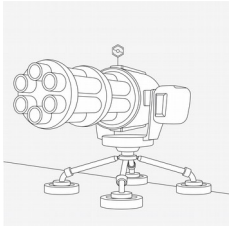
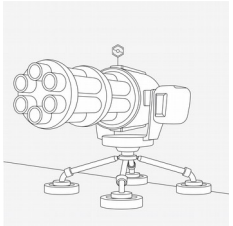
ZeroBS // DDOS Attacker-Capabilities-Scoring



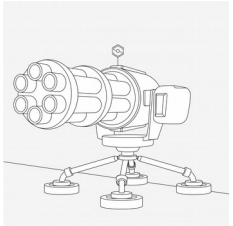
	DRS 1	DRS 2	DRS 3	DRS 4	DRS 5	DRS 6	DRS 7
Name (*)	Poking	ScriptKiddie	Basic Level	Sophisticated	Advanced	Extreme	State Sponsored
Persistance	minutes	hours	hours	days	weeks	weeks	weeks
OSINT + Recon, Snipering					Basic	Full	Full
Can follow DNS/IP-Changes					y	y	y
Can find and record the origin					y	y	Y
Attacks with least necessary ammount / Deep understanding on protection-solutions					y	y	Y
Monitors and reacts on mitigations					y	y	y
Ability to test for whitelists/blacklist (GeoIP)						y	Y

TLP:GREEN

ZeroBS // DDOS Attacker-Capabilities-Scoring



Ability to limit attacks from geo-Ranges						y	y
Ressources/ week if to be rented	1 $	10 $	50 $	500 $	10000 $	No limits	No limits
Smokescreening						y	Y
Multi Vol +L7					y	y	y
CarpetBombing UDP/TCP				y	y	y	y
Unusual Vectors *)					y	y	y
Attack blends into usual traffic (L7)					y	y	y
Botnet for rent/buy		y	y	y			
Operates own botnet					y	y	y
Botnet-Size (AVG, but YMMV)	1	50	5.000	10.000	50.000	500.000	unlimited
Full Browser/Client-capabilities					y	y	y



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)

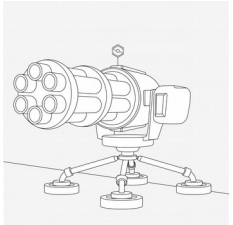
Level 4 // Sophisticated
- That Guy in the Basement with knowledge [1]
- DDoS-Gangs for Rent, the cheaper ones [1]
- minimum-Level for basically all ECommerce-Applications

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

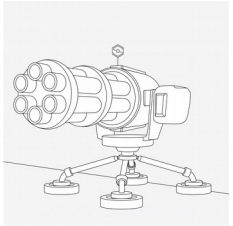
Version 2.8 - 2021-06-04



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