METHODOLOGIE – Lieber einen Service als das ganze Netz verlieren

Nr.	DRS	Layer	Angriffsart	Größe/ IPs	ASNs	Traffic/Request pro IP ***	Pattern	Verteidigungsmethoden											
								1	2	3	4	5	6	7	8	9	10	11	12
1.1	1	3/4	Poking: Traffic von einer IP aus via Trafficgenerator (UDP/TCP)	1	1	hoch	gleich	x			x	x	x	x	x	x	x	x	
1.2	1	7	Poking: Random Requests gegen eine Webapplikation	1	1	hoch	variabel	x						x			x	x	
2.1	2	3/4	TCP/UDP-Floods, einzelne IPs	10	1-2	hoch	gleich	x		x	x	x		x	x	x			
2.2	2	7	HTTP-Requests, einzelne IPs *	10	1-2	hoch	gleich	x		x	x	x		x	x	x			
3.1	3	3/4	TCP/UDP-Floods, mini- Botnet	200	> 10	mittel-hoch	gleich	x		x	x	x		x	x	x			
3.2	3	7	Wordpress-Botnet *	5000	> 10	mittel	gleich	x		x			x			x			x
3.3	3	7	Kleines Botnet oder Booter-Service *	1000	> 10	mittel-hoch	variabel	x		x			x			x			x
3.5	3	3/4	Kleines Botnet oder Booter-Service *	1000	> 10	mittel-hoch	variabel	x		x	x	x	x	x	x	x	x	x	
4.1	4/5	7	Mirai via Darknet, Web	50.000	> 30	mittel	variabel			x	x		x			x	x	x	
4.2	4/5	7	Mirai via Darknet, DNS	50.000	> 30	mittel	variabel				x			x	x		x	x	
4.3	4	3/4	rDDoS klein (< 100 GB oder Netz nicht gesättigt)	1000	> 10	hoch-extrem	gleich			x	x	x		x	x		x	x	
5.1	5	3/4	rDDoS mittel (> 500 GB)	1000	> 30	hoch-extrem	gleich							x	x				
6.1	6/7	3/4	rDDoS Hugh Mongus > 1TB	100.000+	> 100	hochextrem	gleich							x	x				
6.2	6	7	Dorian Grey	200.000	> 1000	niedrig-extrem	variabel						x			x			
6.3	6/7	7	Dyn	40.000	> 30	hoch-extrem	gleich							x					x
6.4	6/7	7	Brian Krebs/Akamai	80.000	> 100	hoch-extrem	variabel							x		x			

Mail ddos@zero.bs

zeroBS

SecurITy made in Germany

LEGENDE

	Ausreichender Schutz
	Schutz kann ggfs versagen (eher ja, aber)
	Schutz nur bedingt gewährleistet (eher nein, kann aber funktionieren)

*) halbintelligente Bots (Random URL, wechselnde User-Agents, keine Redirects/Cookies)

**) Anzahl Bots / IPs

***)

Traffic/Requests	Traffic/Sekunde per IP	Requests/Sekunde per IP
Niedrig	1 MBit/s	10
Mittel	10 MBit/s	100
Hoch	100 MBit/s	1000
Extrem	> 100 MBit/s	> 1000

Mail ddos@zero.bs

APPENDIX

Changelog

Version	Datum	Bearbeiter	RMKS
1.0	2018-06-10	dh	Analysemethodologie verfeinert
0.8	2018-05-22	dh	Weitere Angriffsarten
0.4	2017-05-22	dh	Weitere Angriffsarten
0.1	2016-05-18	mm	Initale Version