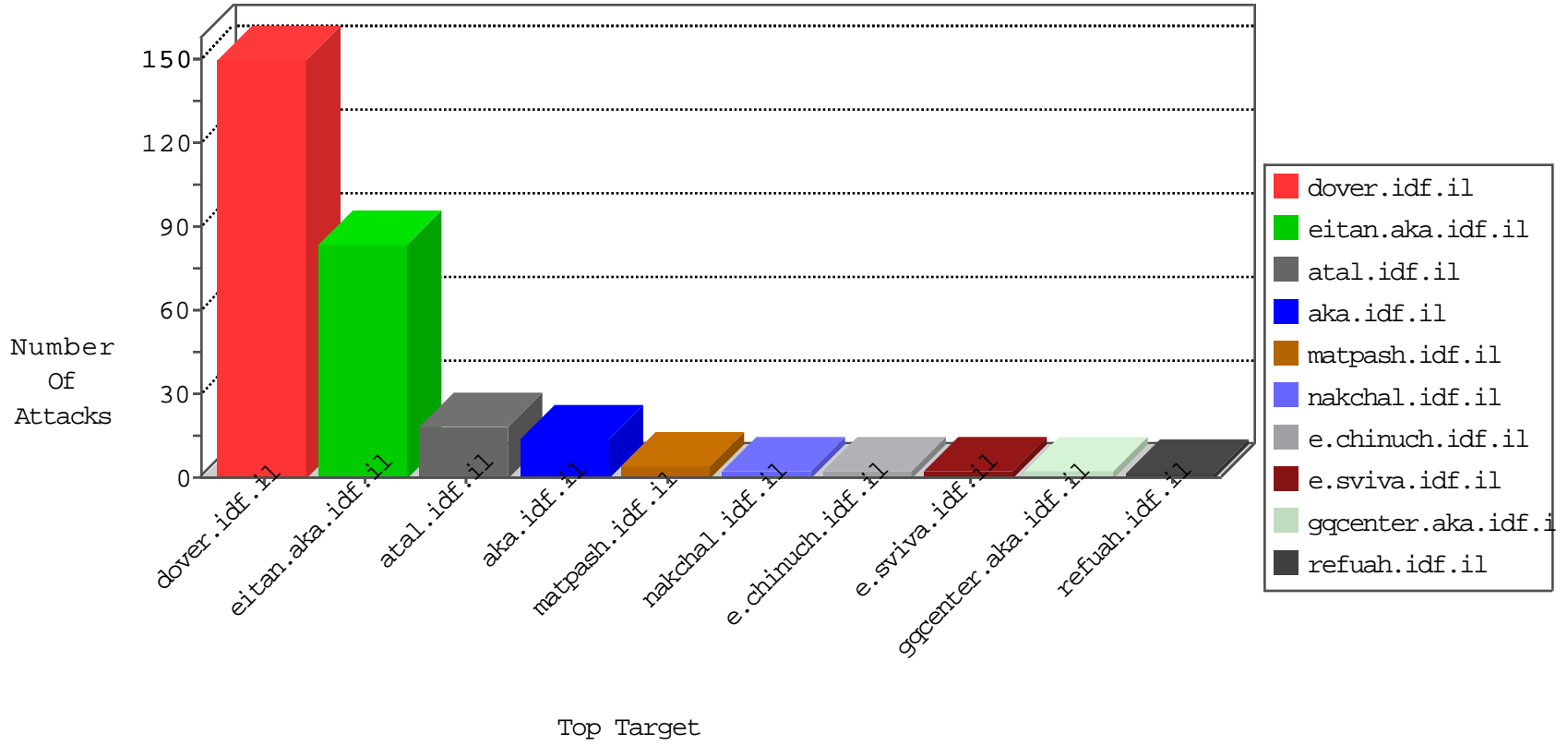


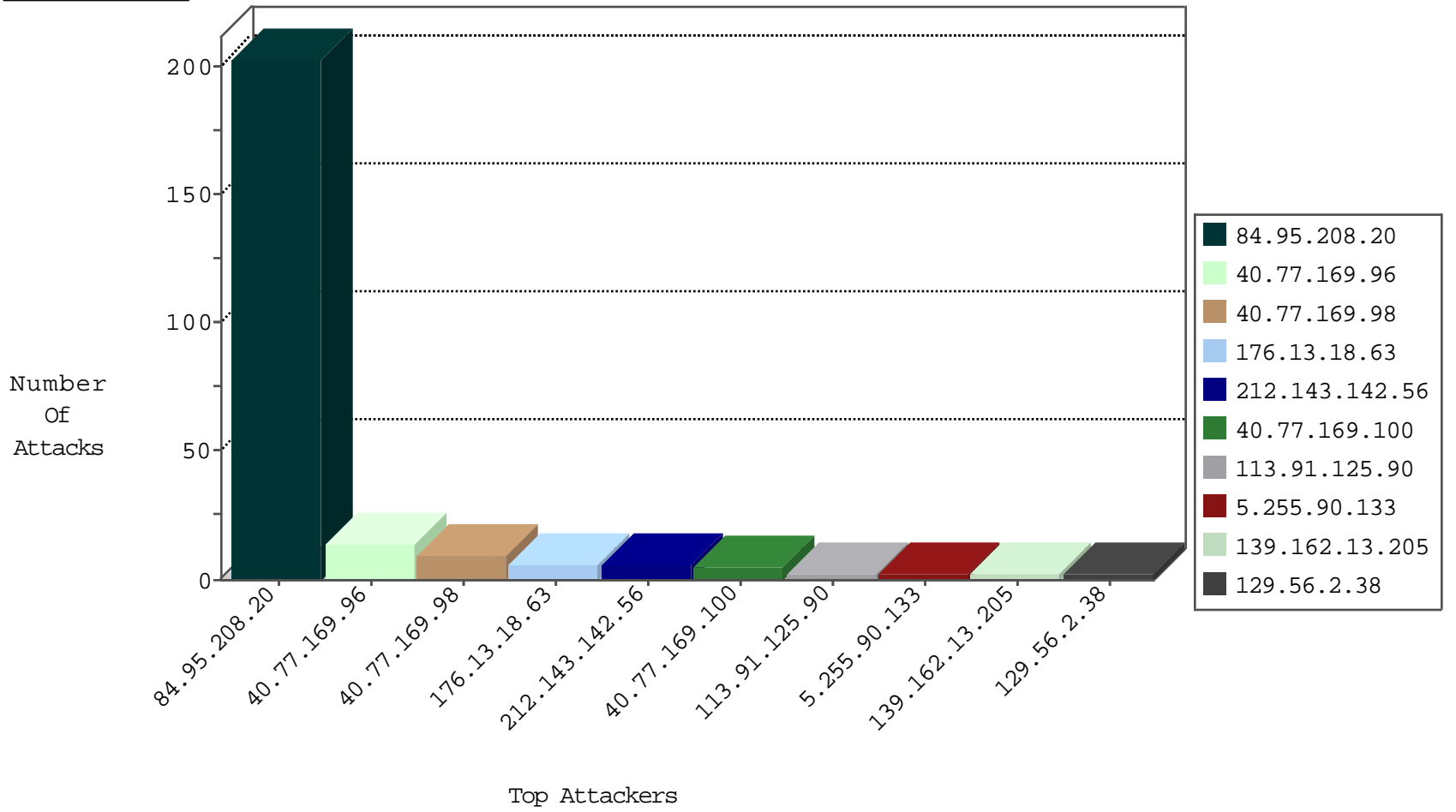
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
222.186.21.95	China	147.237.76.196	e.sviva.idf.il	JLM_Purple_Con_Limit_Http	drop	1
124.190.29.170	Australia	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
88.198.16.153	Germany	147.237.77.216	dover.idf.i	C1000074: HTTP: majestic bot	Permit	2
52.50.60.62	Ireland	147.237.72.166	aka.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.155.58.28	147.237.76.199	Indonesia	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
133.242.4.52	147.237.77.226	Japan	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
133.208.21.66	147.237.76.198	Japan	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
129.56.2.38	147.237.77.179	Nigeria	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.93.137	147.237.77.233	Europe	atal.idf.il	ET SCAN NMAP -sA (2)	1
8.26.94.207	147.237.0.34	Canada	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
5.255.90.133	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
180.97.75.130	147.237.8.46	China	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
133.242.3.168	147.237.76.202	Japan	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
129.56.2.38	147.237.77.235	Nigeria	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.93.140	147.237.77.233	Europe	atal.idf.il	ET SCAN NMAP -sA (2)	1
46.172.71.251	147.237.76.196	Ukraine	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
5.255.90.133	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
40.77.169.96	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	14
40.77.169.98	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	9
176.13.18.63	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
84.95.208.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
40.77.169.100	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
157.55.39.110	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
141.212.122.28	United States	147.237.76.148	ggcenter.aka.idf.il	drop		drop	1
141.212.122.29	United States	147.237.76.148	ggcenter.aka.idf.il	drop		drop	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
82.205.106.236	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	96
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	84
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	8
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	6
207.46.13.34	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
113.91.125.90	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 113.91.125.90	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
40.77.169.101	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	1
139.162.13.205	Singapore	147.237.76.31	nakchal.idf.il	Illegal Byte Code Character in Method	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
46.4.15.197	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
66.249.75.24	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/3142.jpg	Block	1
139.162.13.205	Singapore	147.237.76.31	nakchal.idf.il	NULL Character in Method	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
66.249.75.64	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-21147-he/dover.aspx	Block	1
40.77.169.97	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
157.55.39.24	United States	147.237.72.166	aka.idf.il	Unknown Parameter pagenum in aka.idf.il/chamatz/faq/default.asp	None	1
66.249.64.56	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1245-he/atal.aspx	Block	1
113.91.125.90	China	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
66.249.75.75	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1129-he/dover.aspx	Block	1
40.77.169.99	United States	147.237.77.176	matpash.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
157.55.39.24	United States	147.237.72.166	aka.idf.il	Unknown Parameter pagenum in aka.idf.il/chinuch/gallery/	None	1
66.249.64.60	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1243-he/atal.aspx	Block	1