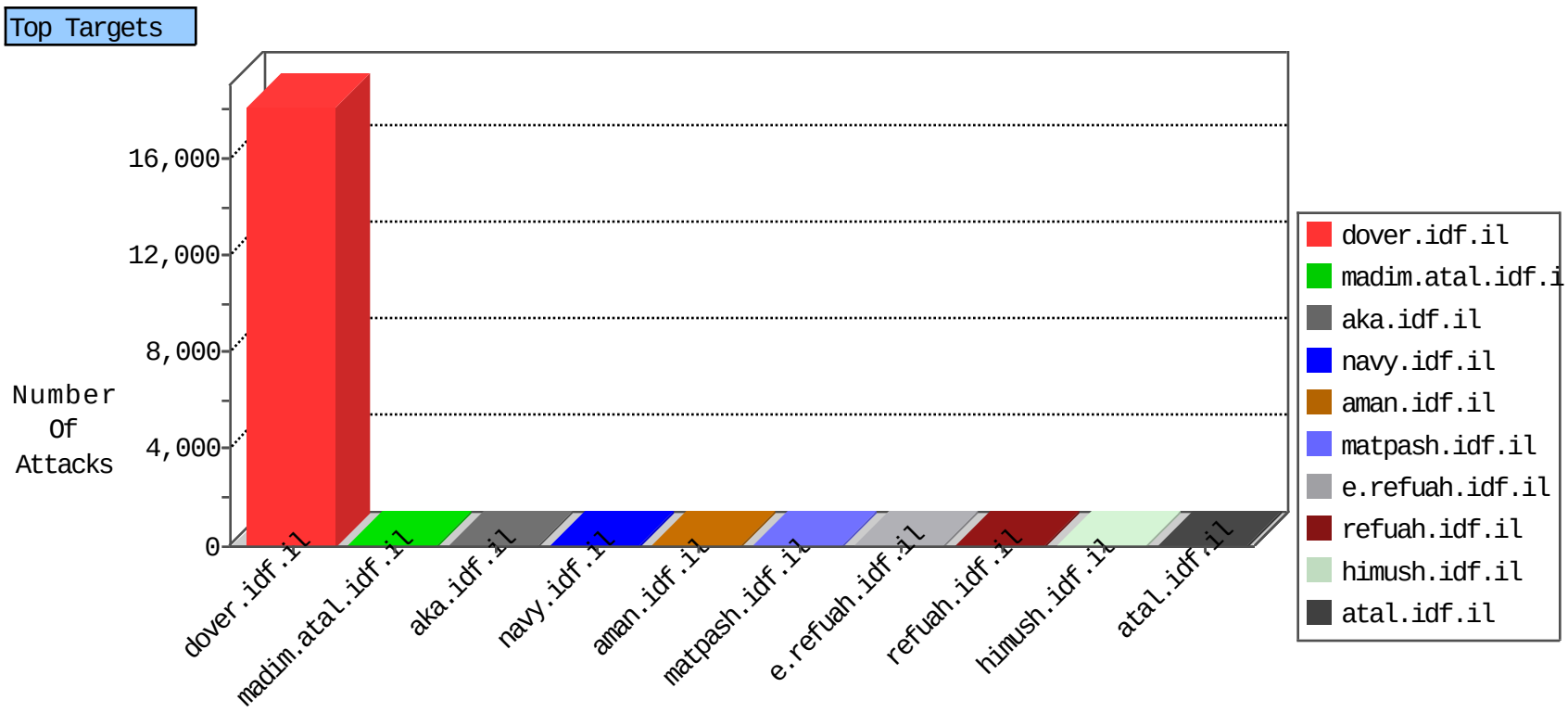
08-26-2016-07:04:05 to 08-26-2016-08:04:05

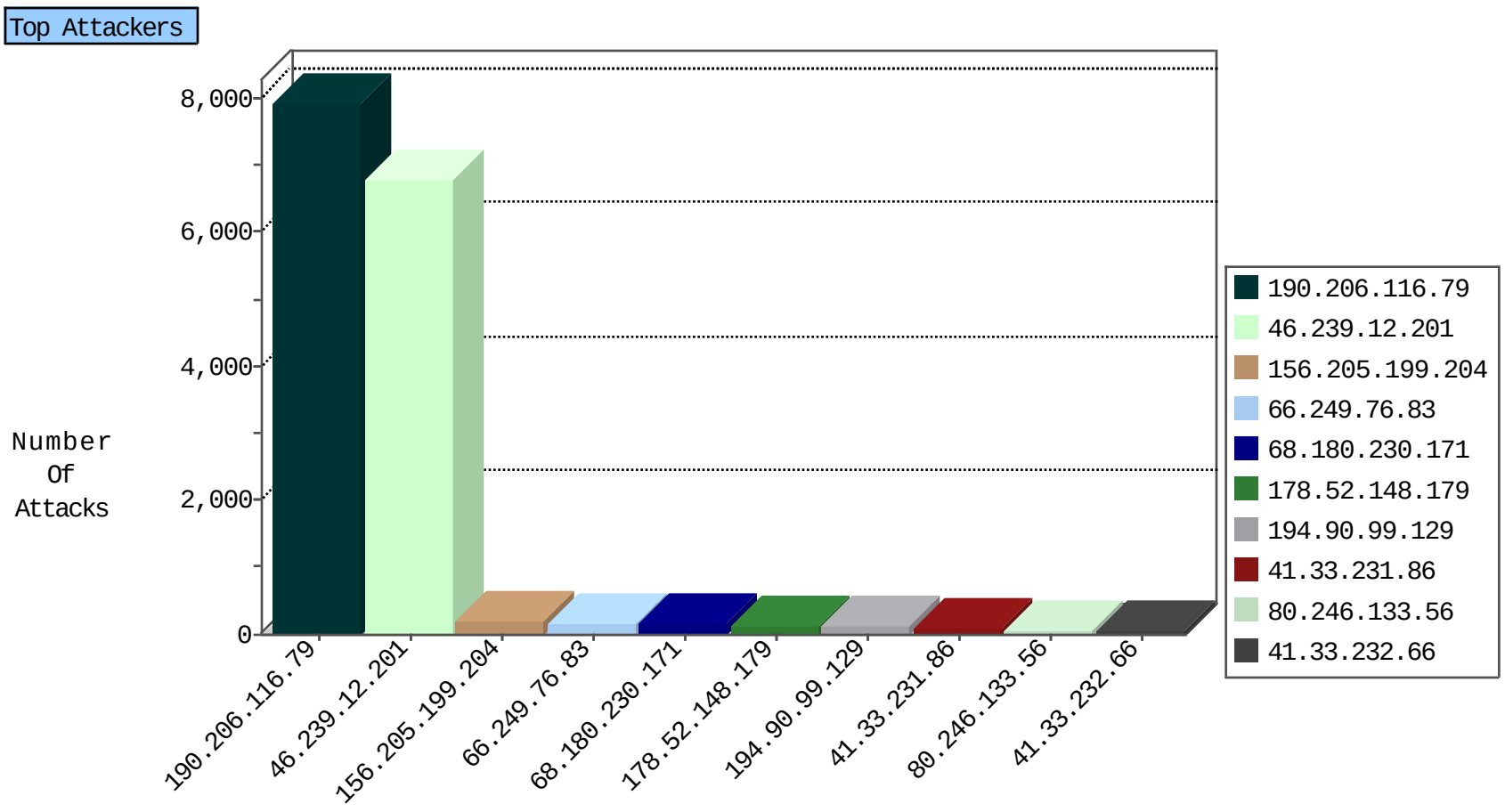
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

08-26-2016-07:04:05 to 08-26-2016-08:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	159910
190.206.116.79	Venezuela	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	79735
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	50991
190.206.116.79	Venezuela	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	42237
178.52.148.179	Syrian Arab Republic	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	177
66.249.76.83	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	165
194.90.99.129	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	116
156.205.199.204	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	116
68.180.230.171	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	95
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	92
156.205.199.204	Egypt	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	72
68.180.230.171	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	68
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	60
37.26.149.241	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	42
136.160.90.51	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	40
80.246.133.56	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	40
109.226.40.40	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	39
87.69.39.186	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	39
139.162.216.112	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	38
66.249.66.177	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	37
157.55.39.93	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	31
50.87.144.145	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	30
109.253.241.15	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	29
181.104.10.6	Argentina	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	27
104.249.236.166	Canada	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	26
192.249.66.247	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	25
72.9.148.10	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	23
157.55.39.194	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	21
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	21
173.247.195.172	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	20
104.158.35.213	Canada	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	20
79.181.242.85	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	20
80.246.133.56	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	20
85.250.147.188	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
79.181.242.85	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
157.55.39.181	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	17
72.9.148.10	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	17
40.77.169.101	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	17
212.235.113.178	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	16
89.139.106.96	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	16
157.55.39.181	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	15
79.181.106.173	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	14
157.55.39.93	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	14
37.26.148.253	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	14
85.65.223.236	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
94.71.100.80	Greece	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
192.249.66.247	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
52.0.104.143	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
104.249.236.166	Canada	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
40.77.169.101	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12

08-26-2016-07:04:05 to 08-26-2016-08:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

08-26-2016-07:04:05 to 08-26-2016-08:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
163.172.169.150	147.237.8.50	United Kingdom	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
46.227.67.172	147.237.76.44	Sweden	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
87.236.194.161	147.237.77.227	Czech Republic	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
23.94.102.8	147.237.0.19	United States	madim.atal.idf.il	WEB-CGI redirect access	1

08-26-2016-07:04:05 to 08-26-2016-08:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.239.12.201	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6360
46.239.12.201	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop		drop	450
190.206.116.79	Venezuela	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	210
89.187.219.147	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
40.77.169.96	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	22
40.77.169.99	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	14
178.52.148.179	Syrian Arab Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
40.77.169.100	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
66.102.9.171	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
40.77.169.99	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
131.253.25.192	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.120.129.196	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
80.246.133.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
136.160.90.51	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
157.55.39.181	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
184.105.247.239	United States	147.237.0.200	m4u.idf.il	drop		drop	1
89.189.67.190	Yemen	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
157.55.39.194	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
100.92.245.253		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1

08-26-2016-07:04:05 to 08-26-2016-08:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.116.5.146	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
46.19.85.129	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
109.253.203.27	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	3
185.32.179.180	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.249.64.158	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/robots.txt	Block	1
40.77.169.101	United States	147.237.77.176	matpash.idf.il	Illegal Byte Code Character in URL /1328-en/cogat.aspx#011404	Block	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/main/giyus/general.aspx	Block	1
54.225.80.243	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/miluim/about.aspx	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	PHP Attempt	Block	1
66.249.69.13	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
40.77.169.101	United States	147.237.77.176	matpash.idf.il	Multiple Illegal Byte Code Character in URL from 40.77.169.101	Block	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/main/smalim/showbig.aspx	Block	1
65.78.15.8	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.249.76.47	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/kamlar/adv.asp	Block	1
66.249.76.113	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/lomdim/bakashot/abroad/default.asp	Block	1
66.249.64.105	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/mobile/main/giyus/general.aspx	Block	1
180.76.15.21	China	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.76.109	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.109	Block	1
68.180.229.49	United States	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	1
66.249.64.105	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/mobile/main/smalim/showbig.aspx	Block	1
5.18.85.207	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/mobile/main/giyus/general.aspx	Block	1
46.150.97.94	Ukraine	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1

08-26-2016-07:04:05 to 08-26-2016-08:04:05