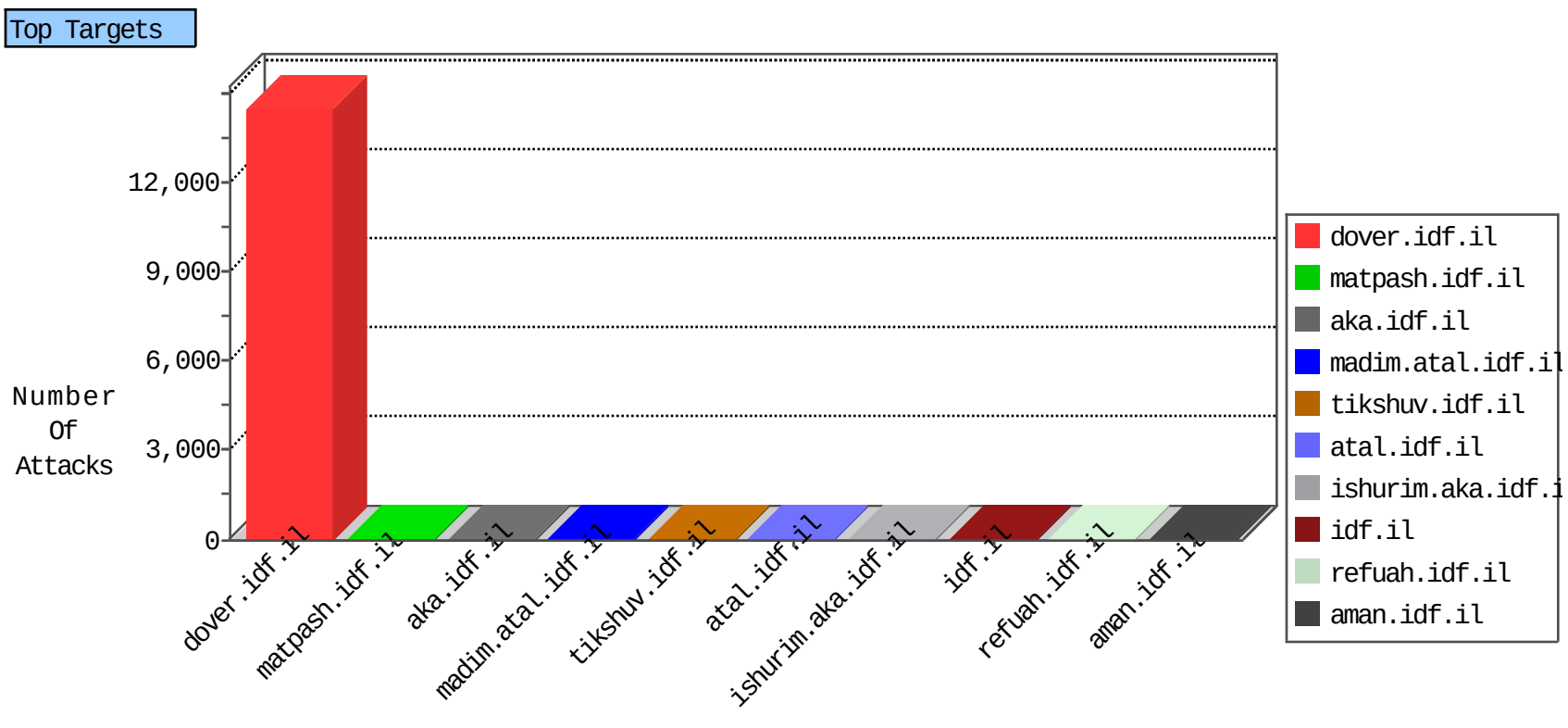
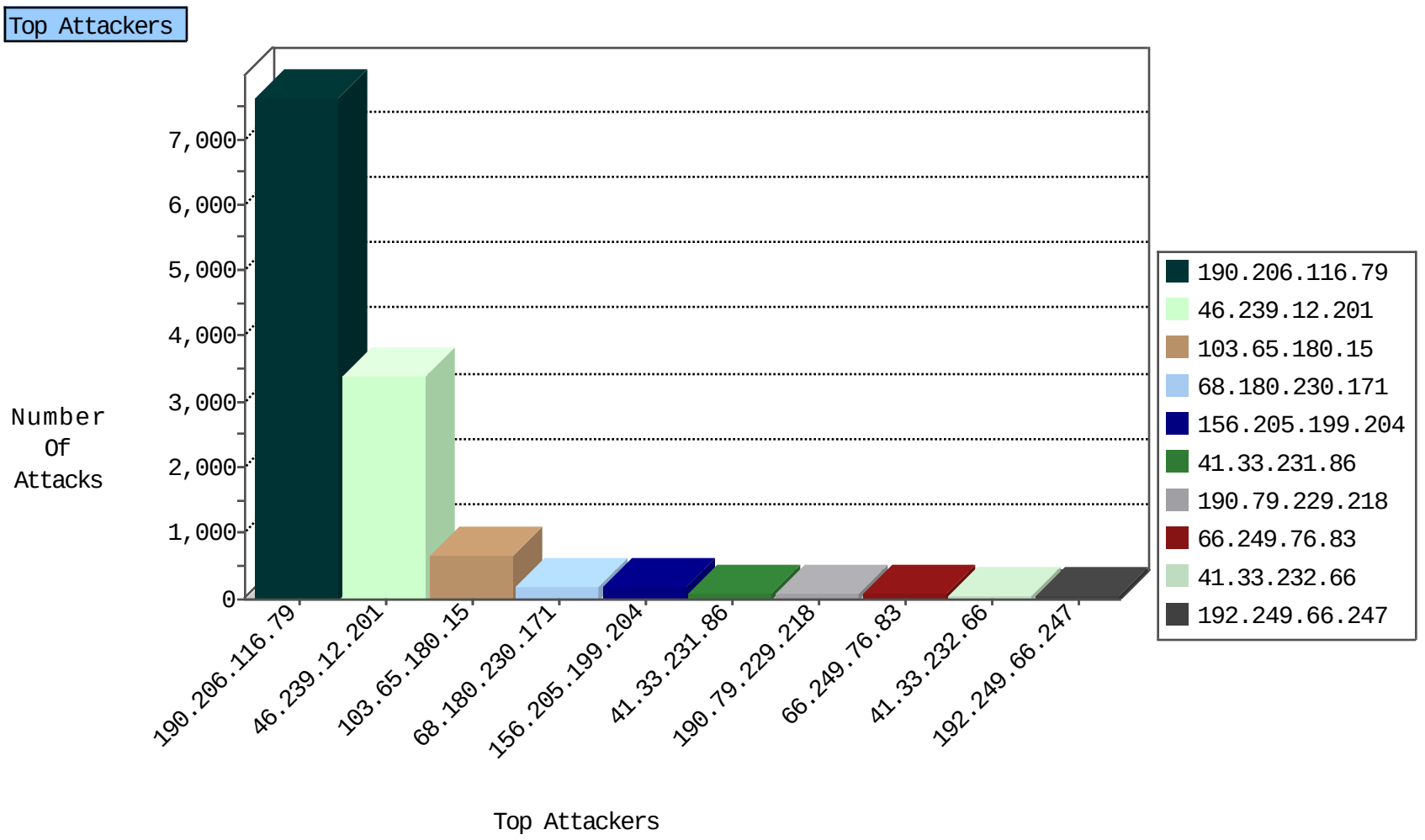
08-26-2016-06:04:05 to 08-26-2016-07:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-26-2016-06:04:05 to 08-26-2016-07:04:05

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	145749
190.206.116.79	Venezuela	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	67530
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	59322
190.206.116.79	Venezuela	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	56428
103.65.180.15		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	709
68.180.230.171	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	143
156.205.199.204	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	114
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	86
156.205.199.204	Egypt	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	72
66.249.76.83	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	72
190.79.229.218	Venezuela	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	60
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	58
68.180.230.171	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	48
50.87.144.145	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	45
66.249.69.14	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	40
192.249.66.247	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	39
109.226.40.40	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	35
217.132.34.85	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	27
157.55.39.181	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	27
139.162.216.112	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	26
157.55.39.194	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	26
157.55.39.93	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	25
109.67.114.186	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	24
80.246.133.235	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	22
157.55.39.181	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	22
157.55.39.194	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	20
157.55.39.181	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	22
157.55.39.194	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	20
74.97.177.80	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	20
136.160.90.51	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	19
66.199.72.220	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
109.66.138.208	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
157.55.39.93	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
5.22.135.146	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
72.9.148.10	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	17
66.249.66.177	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	16
66.249.69.22	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	16
72.9.148.10	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	16
37.26.149.169	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	14
190.79.229.218	Venezuela	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	14
80.246.133.235	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
79.179.114.85	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
40.77.169.98	United States	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
79.182.20.69	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
162.243.253.50	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
40.77.169.101	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
159.220.75.2	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
109.253.229.110	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
40.77.169.97	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	9
159.220.75.3	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8
66.249.76.85	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8

08-26-2016-06:04:05 to 08-26-2016-07:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

08-26-2016-06:04:05 to 08-26-2016-07:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
50.116.123.135	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
220.231.195.122	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN NMAP -sS window 4096	1
163.172.169.150	147.237.0.34	United Kingdom	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
122.72.53.188	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
84.54.72.35	147.237.77.170	Uzbekistan	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
50.116.123.135	147.237.76.42	United States	refuah.idf.il	ET SCAN Potential SSH Scan	1
50.116.123.135	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
220.231.195.122	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.169.150	147.237.0.33	United Kingdom	idf.il	ET SCAN NMAP -sS window 1024	1
122.72.53.188	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
66.249.64.108	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	1

08-26-2016-06:04:05 to 08-26-2016-07:04:05

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	3249
46.239.12.201	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop		drop	150
167.220.232.104	Japan	147.237.77.216	dover.idf.il	drop	SAM rule	drop	22
40.77.169.101	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	18
40.77.169.97	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
40.77.169.99	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	16
40.77.169.96	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	10
40.77.169.99	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	10
40.77.169.103	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
40.77.169.103	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	3
40.77.169.97	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
46.165.197.142	Germany	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
40.77.169.96	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
139.162.13.205	Singapore	147.237.77.233	atal.idf.il	drop	SAM rule	drop	1
51.9.115.59	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

08-26-2016-06:04:05 to 08-26-2016-07:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.203.27	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
66.249.76.109	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/900-he/chinuch.aspx	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.64.133	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
73.140.87.223	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
66.249.69.22	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1733	Block	1
77.139.62.222	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.106	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to www.kosher-kravi.idf.il/default.aspx	Block	1
40.77.167.50	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/robots.txt	Block	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/qiyus/qeneral/default.a	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
66.249.64.58	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1

08-26-2016-06:04:05 to 08-26-2016-07:04:05