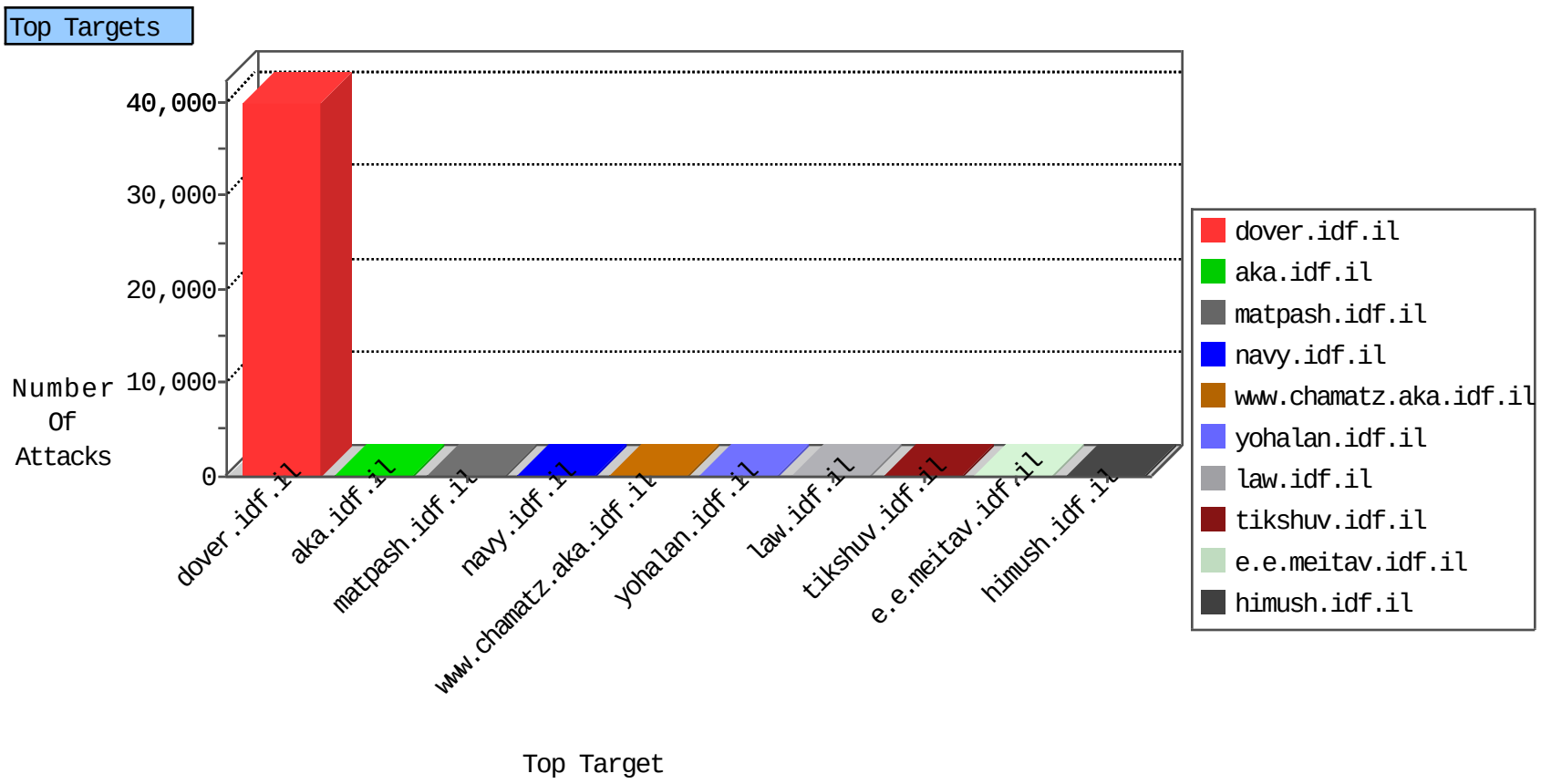
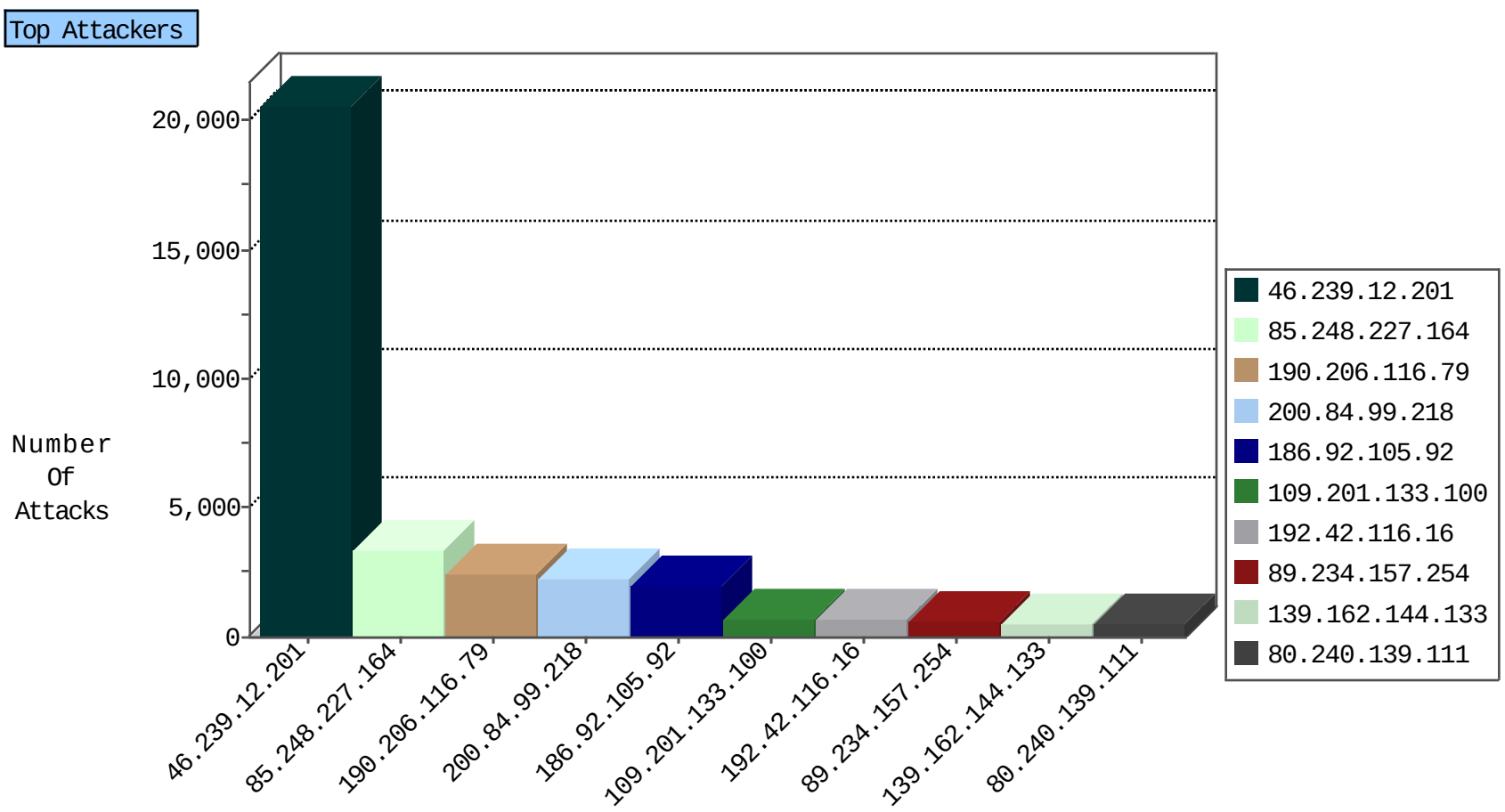
08-26-2016-02:04:09 to 08-26-2016-03:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-26-2016-02:04:09 to 08-26-2016-03:04:09

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	network flood IPv4 TCP-FIN-ACK	drop	3255199
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	437951
200.84.99.218	Venezuela	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	1367
190.206.116.79	Venezuela	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	1229
190.206.116.79	Venezuela	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1207
186.92.105.92	Venezuela	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1124
200.84.99.218	Venezuela	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	930
186.92.105.92	Venezuela	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	884
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	535
62.210.37.82	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	350
62.210.37.82	France	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	297
186.94.218.214	Venezuela	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	278
186.88.195.95	Venezuela	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	271
186.93.193.132	Venezuela	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	256
68.180.230.171	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	231
109.226.40.40	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	200
186.88.195.95	Venezuela	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	199
62.210.37.82	France	147.237.77.216	dover.idf.il	DOS-HTTP-torshammer	forward	181
37.238.166.152	Iraq	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	145
68.180.230.171	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	116
136.160.90.51	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	105
5.28.189.100	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	83
156.205.199.204	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	82
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	80
186.94.218.214	Venezuela	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	79
139.162.216.112	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	77
50.87.144.145	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	77
66.249.69.14	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	74
156.205.199.204	Egypt	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	68
130.216.95.217	New Zealand	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	45
104.249.236.166	Canada	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	39
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	37
185.120.125.115	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	32
130.216.95.217	New Zealand	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	31
157.55.39.93	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	30
37.26.146.188	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	29
40.77.169.98	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	28
157.55.39.181	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	28
202.36.244.4	New Zealand	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	27
5.22.132.9	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	26
41.34.203.1	Egypt	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	24
157.55.39.37	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	23
52.0.104.143	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	23
157.55.39.181	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	21
66.249.69.18	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	21
159.220.75.3	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	21
159.220.75.2	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	20
192.249.66.247	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	20
195.57.139.13	Spain	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	20
109.65.102.33	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	20

08-26-2016-02:04:09 to 08-26-2016-03:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
193.111.140.106	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	4
85.14.244.98	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
36.110.147.71	China	147.237.77.74	law.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

08-26-2016-02:04:09 to 08-26-2016-03:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
18.85.22.237	147.237.77.74	United States	law.idf.il	Tehila - Perl LWP with fake user agent	2
163.172.169.150	147.237.8.28	United Kingdom	e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
183.129.160.229	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
163.172.169.150	147.237.77.212	United Kingdom	e.dover.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
94.102.48.195	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
201.238.202.219	147.237.76.38	Chile	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.169.150	147.237.77.227	United Kingdom	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5800-5820	1

08-26-2016-02:04:09 to 08-26-2016-03:04:09

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	20202
85.248.227.164	Slovakia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3359
192.42.116.16	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	710
109.201.133.100	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	703
89.234.157.254	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	634
139.162.144.133	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	521
80.240.139.111	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	491
46.239.12.201	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop		drop	400
212.34.12.166	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	192
212.34.11.97	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	187
178.79.63.8		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	131
185.29.9.249	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
37.238.166.152	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
40.77.169.103	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	18
167.220.232.104	Japan	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
40.77.169.99	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	9
46.120.129.196	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
40.77.169.96	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	7
40.77.169.101	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
40.77.169.103	United States	147.237.76.86	navy.idf.il	drop	SAM rule	drop	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
40.77.169.101	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	5
40.77.169.99	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	4
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.210	Israel	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	2
139.162.37.113	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
77.120.125.248	Ukraine	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	1
31.13.102.105	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	1
40.77.169.99	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
31.13.102.116	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.i	drop	SAM rule	drop	1
141.212.122.100	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	1
169.229.3.91	United States	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	1
128.242.249.11	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.101	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
169.229.3.91	United States	147.237.77.121	e.navy.idf.il	drop	SAM rule	drop	1

08-26-2016-02:04:09 to 08-26-2016-03:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.229.65.111	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	4
80.240.139.111	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	3
157.55.39.109	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
77.124.57.70	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/oprolescategory/oprolescategory.in.aspx	Block	1
81.149.238.182	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/chamatz	Block	1
31.168.20.242	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
193.111.136.162	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
77.139.141.39	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
66.102.9.85	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
79.178.13.239	Israel	147.237.76.30	himush.idf.il	Multiple Unauthorized URL Access from 79.178.13.239	Block	1
85.248.227.164	Slovakia	147.237.77.216	dover.idf.il	NULL Character in Method	Block	1
66.249.75.174	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	1
79.178.13.239	Israel	147.237.76.30	himush.idf.il	Unauthorized HTTP Method	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/main/stm	Block	1
68.180.228.231	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-he/cogat.aspx	Block	1

08-26-2016-02:04:09 to 08-26-2016-03:04:09