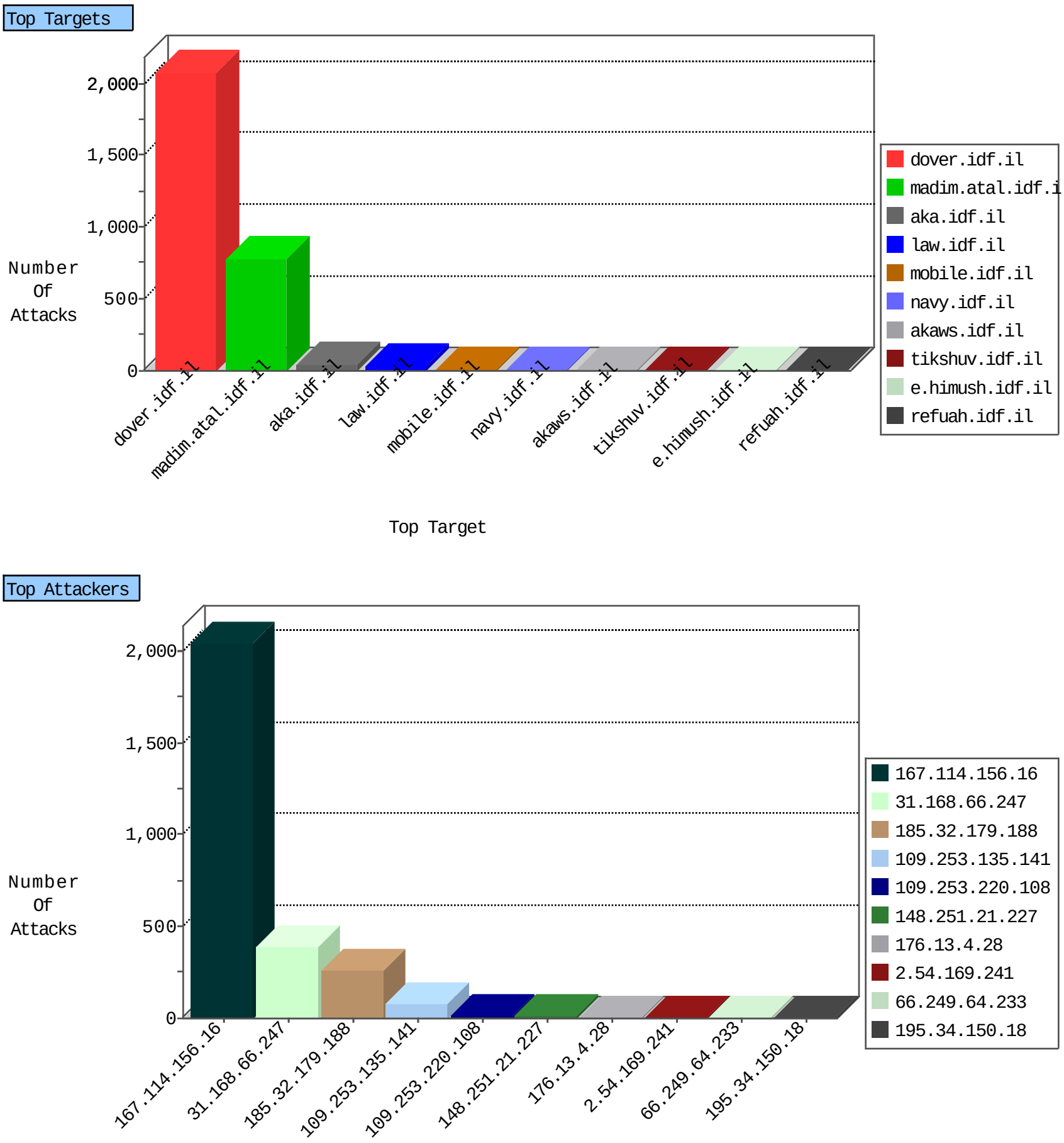
01-05-2016-07:04:07 to 01-05-2016-08:04:07

IDF Under Attack Daily Report



01-05-2016-07:04:07 to 01-05-2016-08:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3164
207.104.161.245	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1

01-05-2016-07:04:07 to 01-05-2016-08:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-05-2016-07:04:07 to 01-05-2016-08:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
185.32.179.188	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	3
194.165.155.114	147.237.76.197	Jordan	e.himush.idf.il	ET SCAN NMAP -sS window 3072	1
180.97.106.37	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
149.78.111.233	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
119.204.0.194	147.237.0.35	Korea, Republic of	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
82.81.3.197	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.146.182	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
194.165.155.114	147.237.76.197	Jordan	e.himush.idf.il	ET SCAN NMAP -sS window 4096	1
180.97.106.36	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
123.189.7.254	147.237.0.35	China	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
82.117.208.243	147.237.77.226		www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.75	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

01-05-2016-07:04:07 to 01-05-2016-08:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.168.66.247	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	183
31.168.66.247	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	178
185.32.179.188	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 185.32.179.188	Block	122
185.32.179.188	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	102
109.253.135.141	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	75
185.32.179.188	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 185.32.179.188	Block	29
31.168.66.247	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	24
109.253.220.108	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	16
148.251.21.227	Germany	147.237.77.74	law.idf.il	Distributed Suspicious Response Code	Block	10
176.13.4.28	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
2.54.169.241	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	5
2.54.186.182	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	4
109.253.207.39	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
176.12.136.79	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
208.115.113.84	United States	147.237.77.74	law.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.110	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.11.80	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
5.28.191.200	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.10.165	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
80.246.139.78	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.12.149.232	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	2
40.77.167.83	United States	147.237.77.74	law.idf.il	Distributed Suspicious Response Code	Block	2
84.109.19.32	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pb_login in www.aka.idf.il/main/giyus/login.aspx	None	2
109.253.194.31	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
77.125.135.112	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general/aspx	Block	2
207.46.13.93	United States	147.237.77.74	law.idf.il	Distributed Suspicious Response Code	Block	2
2.52.132.103	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.9.68	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	2
207.46.13.123	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
109.201.154.239	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
84.110.145.247	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
46.19.85.238	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
185.32.179.188	Israel	147.237.0.19	madim.atal.idf.i	Too Many 404: Response Code per Session	Block	1
80.246.136.63	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.52.165.141	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.207.91	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
66.249.64.153	Israel	147.237.77.74	law.idf.il	Distributed Suspicious Response Code	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
37.26.147.194	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.178.200.21	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.64.238	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.238	Block	1
109.253.131.172	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.250.210.105	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.136.102	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.229.173	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.159	Israel	147.237.77.74	law.idf.il	Distributed Suspicious Response Code	Block	1