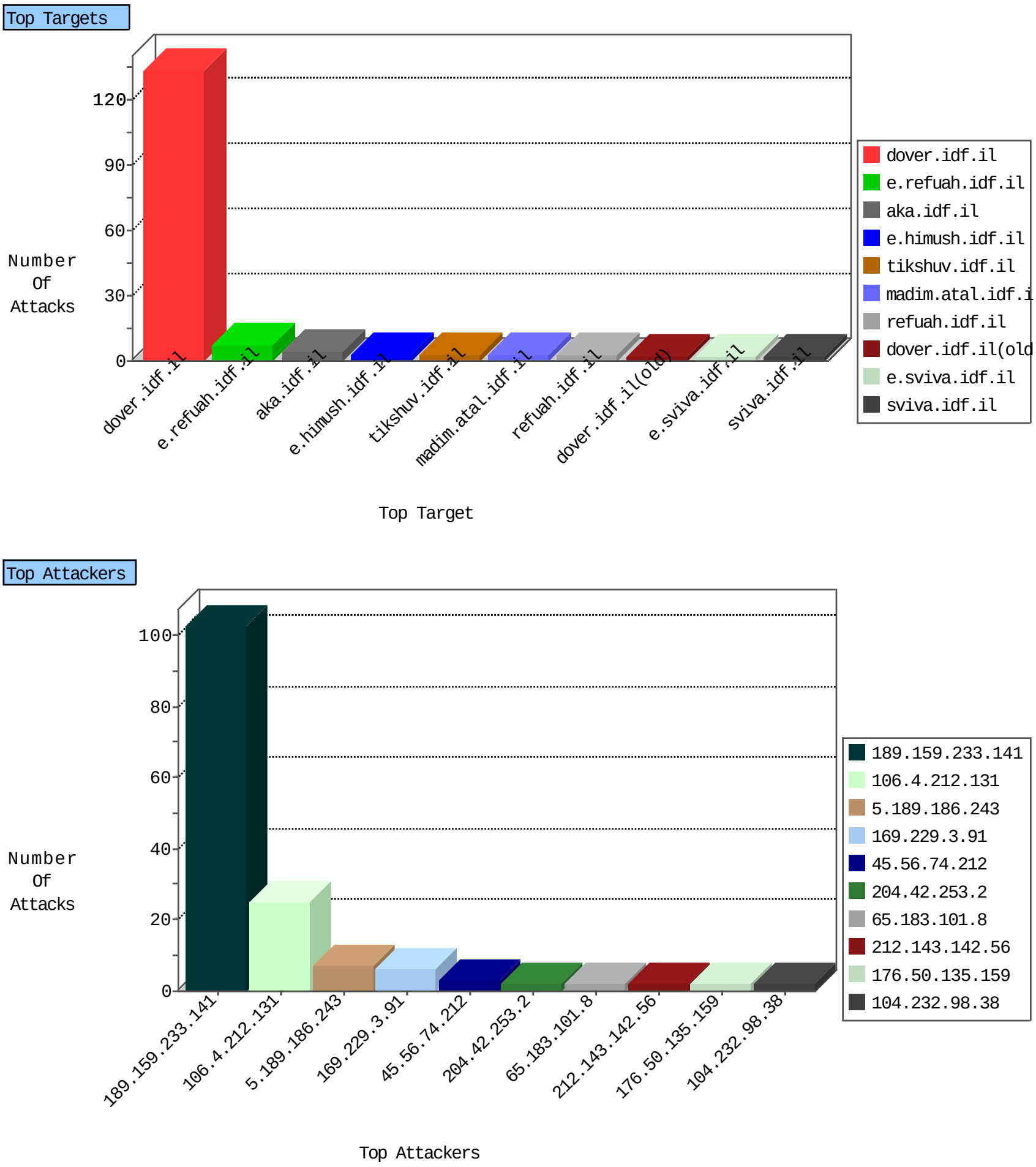
09-02-2016-05:04:09 to 09-02-2016-06:04:09

IDF Under Attack Daily Report



09-02-2016-05:04:09 to 09-02-2016-06:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.189.186.243	Germany	147.237.76.44	e.refuah.idf.il	Black List	drop	3
5.189.186.243	Germany	147.237.76.42	refuah.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.44	e.refuah.idf.il	Black List	drop	2
5.189.186.243	Germany	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1
62.48.35.159	Italy	147.237.0.200	m4u.idf.il	JLM_Purple_Con_Limit_Http	drop	1
5.189.186.243	Germany	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
93.158.200.97	Netherlands	147.237.76.86	navy.idf.il	Black List	drop	1
94.156.128.101	Bulgaria	147.237.76.196	e.sviva.idf.il	Black List	drop	1

09-02-2016-05:04:09 to 09-02-2016-06:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-02-2016-05:04:09 to 09-02-2016-06:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
93.174.93.220	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
65.183.101.8	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 3072	1
45.56.74.212	147.237.76.197	United States	e.himush.idf.il	ET SCAN Potential SSH Scan	1
45.33.116.208	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
198.52.97.89	147.237.77.74	United States	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
176.50.135.159	147.237.0.17	Russian Federation	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
146.185.146.112	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
104.232.98.38	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
65.183.101.8	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 4096	1
45.56.74.212	147.237.77.234	United States	halag.idf.il	ET SCAN Potential SSH Scan	1
45.56.74.212	147.237.76.44	United States	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
5.255.90.133	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
201.38.68.132	147.237.77.226	Brazil	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
198.12.74.76	147.237.0.19	United States	madim.atal.idf.il	WEB-CGI redirect access	1
176.50.135.159	147.237.0.15	Russian Federation	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
104.232.98.38	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 3072	1

09-02-2016-05:04:09 to 09-02-2016-06:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
189.159.233.141	Mexico	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	103
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.77.121	e.navy.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.76.34	yohalan.idf.il	drop	First packet isn't SYN	drop	1
184.105.139.67	United States	147.237.76.197	e.himush.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.76.44	e.refuah.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.76.197	e.himush.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.76.202	e.halag.idf.il	drop	First packet isn't SYN	drop	1

09-02-2016-05:04:09 to 09-02-2016-06:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.4.212.131	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 106.4.212.131	Block	17
106.4.212.131	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	6
106.4.212.131	China	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/default.aspx	Block	1
66.249.66.250	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/navmenu/	Block	1
187.169.188.44	Mexico	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.249.76.121	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1392-en/cogat.asp	Block	1
66.249.76.67	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/robots.txt	Block	1
204.79.180.5	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/home.asp	Block	1
73.22.155.10	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-ar/www.idf.il/ar	Block	1
207.46.13.64	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/kamlar/klali/default.asp	None	1
77.138.240.165	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.138.240.165	Block	1
106.4.212.131	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.asp	Block	1
66.249.76.115	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/894-en	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.64.253	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/news/news.in.aspx	Block	1
157.55.39.97	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
66.249.76.116	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/modules/forums.frm/frmprintmessage.aspx	Block	1

09-02-2016-05:04:09 to 09-02-2016-06:04:09