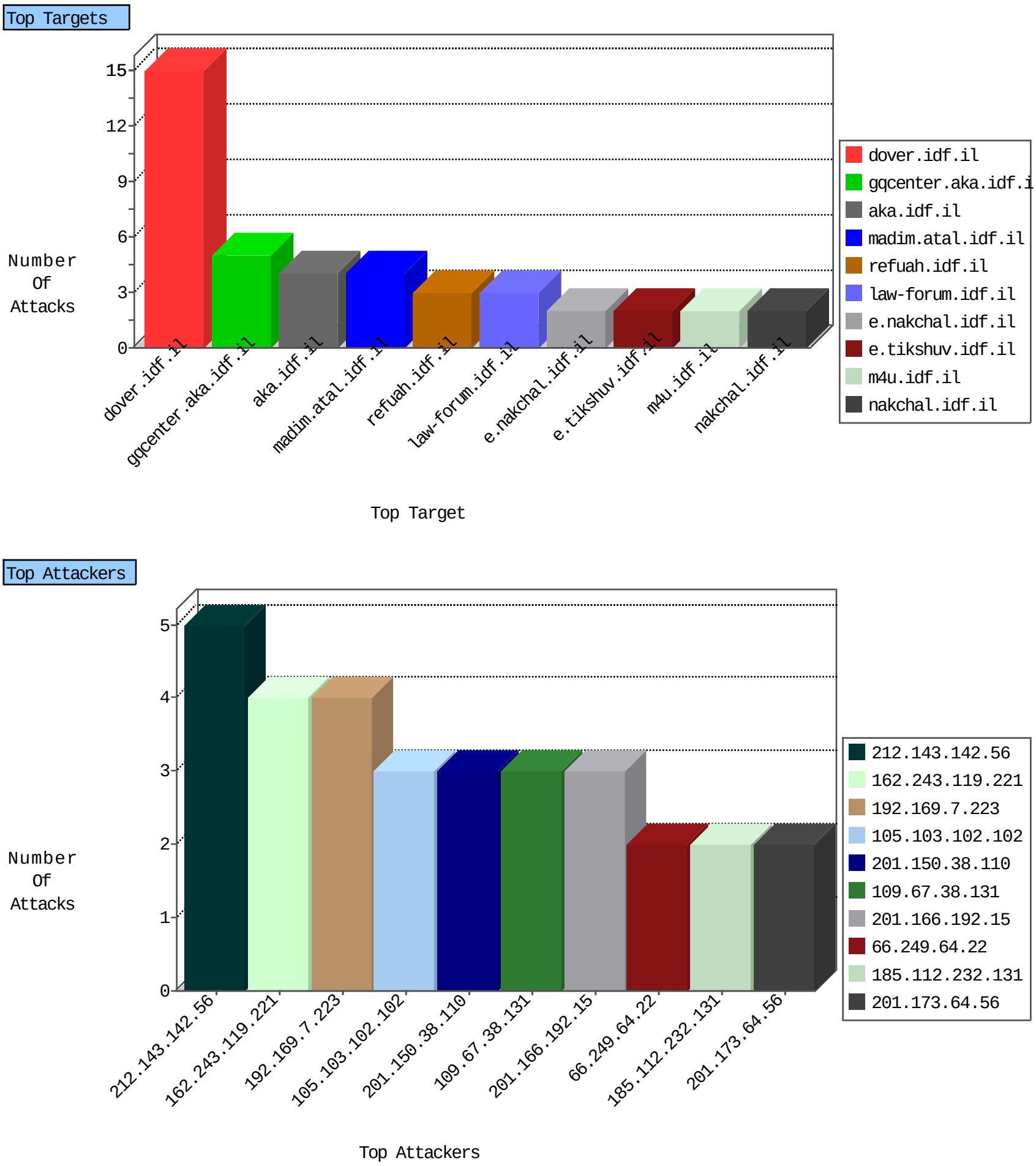
08-31-2016-04:04:01 to 08-31-2016-05:04:01

IDF Under Attack Daily Report



08-31-2016-04:04:01 to 08-31-2016-05:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
178.239.62.141	Netherlands	147.237.76.44	e.refuah.idf.il	Black List	drop	1
91.230.107.174	Russian Federation	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
93.158.200.97	Netherlands	147.237.76.30	himush.idf.il	Black List	drop	1
93.158.200.97	Netherlands	147.237.76.200	eitan.aka.idf.il	Black List	drop	1

08-31-2016-04:04:01 to 08-31-2016-05:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

08-31-2016-04:04:01 to 08-31-2016-05:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
50.116.123.135	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
201.150.38.110	147.237.77.19	Mexico	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
198.167.223.33	147.237.0.16	Saint Kitts and Nevis	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
183.82.106.200	147.237.76.42	India	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
162.243.119.221	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
162.243.119.221	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
92.26.128.195	147.237.76.31	United Kingdom	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
52.74.147.121	147.237.76.199	Singapore	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
201.150.38.110	147.237.77.19	Mexico	law-forum.idf.il	ET SCAN NMAP -sS window 2048	1
201.150.38.110	147.237.77.19	Mexico	law-forum.idf.il	ET SCAN NMAP -f -sS	1
183.82.106.200	147.237.76.42	India	refuah.idf.il	ET SCAN NMAP -sS window 3072	1
163.172.169.150	147.237.8.28	United Kingdom	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
162.243.119.221	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
162.243.119.221	147.237.8.45	United States	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
52.74.147.121	147.237.76.199	Singapore	e.nakchal.idf.il	ET SCAN NMAP -sS window 3072	1

08-31-2016-04:04:01 to 08-31-2016-05:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.169.7.223	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	3
185.112.232.131	Iraq	147.237.72.217	e.idf.il	drop	First packet isn't SYN	drop	2
201.166.192.15	Mexico	147.237.0.35	akaws.idf.il	drop		drop	1
180.97.106.161	China	147.237.76.34	yohalan.idf.il	drop		drop	1
201.166.192.155	Mexico	147.237.0.200	m4u.idf.il	drop		drop	1
79.177.25.32	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
201.173.235.250	Mexico	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
108.74.163.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
118.173.184.142	Thailand	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
201.166.192.15	Mexico	147.237.0.33	idf.il	drop		drop	1
180.97.106.161	China	147.237.0.200	m4u.idf.il	drop		drop	1

08-31-2016-04:04:01 to 08-31-2016-05:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
105.103.102.102	Algeria	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 105.103.102.102	Block	3
109.67.38.131	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
201.173.103.72	Mexico	147.237.77.216	dover.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
189.218.76.221	Mexico	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
50.92.33.221	Canada	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
201.172.27.129	Mexico	147.237.77.170	maarachot.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
203.127.96.198	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
189.218.76.221	Mexico	147.237.0.19	madim.atal.idf.il	Redundant HTTP Headers Content-Type	Block	1
66.249.64.22	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.22	Block	1
201.172.99.57	Mexico	147.237.76.200	eitan.aka.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
157.55.39.97	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
203.127.96.213	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
189.219.138.173	Mexico	147.237.77.74	law.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
66.249.64.22	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
201.173.64.56	Mexico	147.237.76.30	himush.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
187.160.235.217	Mexico	147.237.76.147	chinuch.aka.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
219.75.81.197	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
192.169.7.223	United States	147.237.76.42	refuah.idf.il	Unauthorized Method HEAD for 147.237.76.42/	Block	1
66.249.66.176	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
201.173.64.56	Mexico	147.237.76.31	nakchal.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
187.161.240.151	Mexico	147.237.77.176	matpash.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
201.166.192.15	Mexico	147.237.0.34	tikshuv.idf.il	Redundant HTTP Headers Content-Type	Block	1

08-31-2016-04:04:01 to 08-31-2016-05:04:01