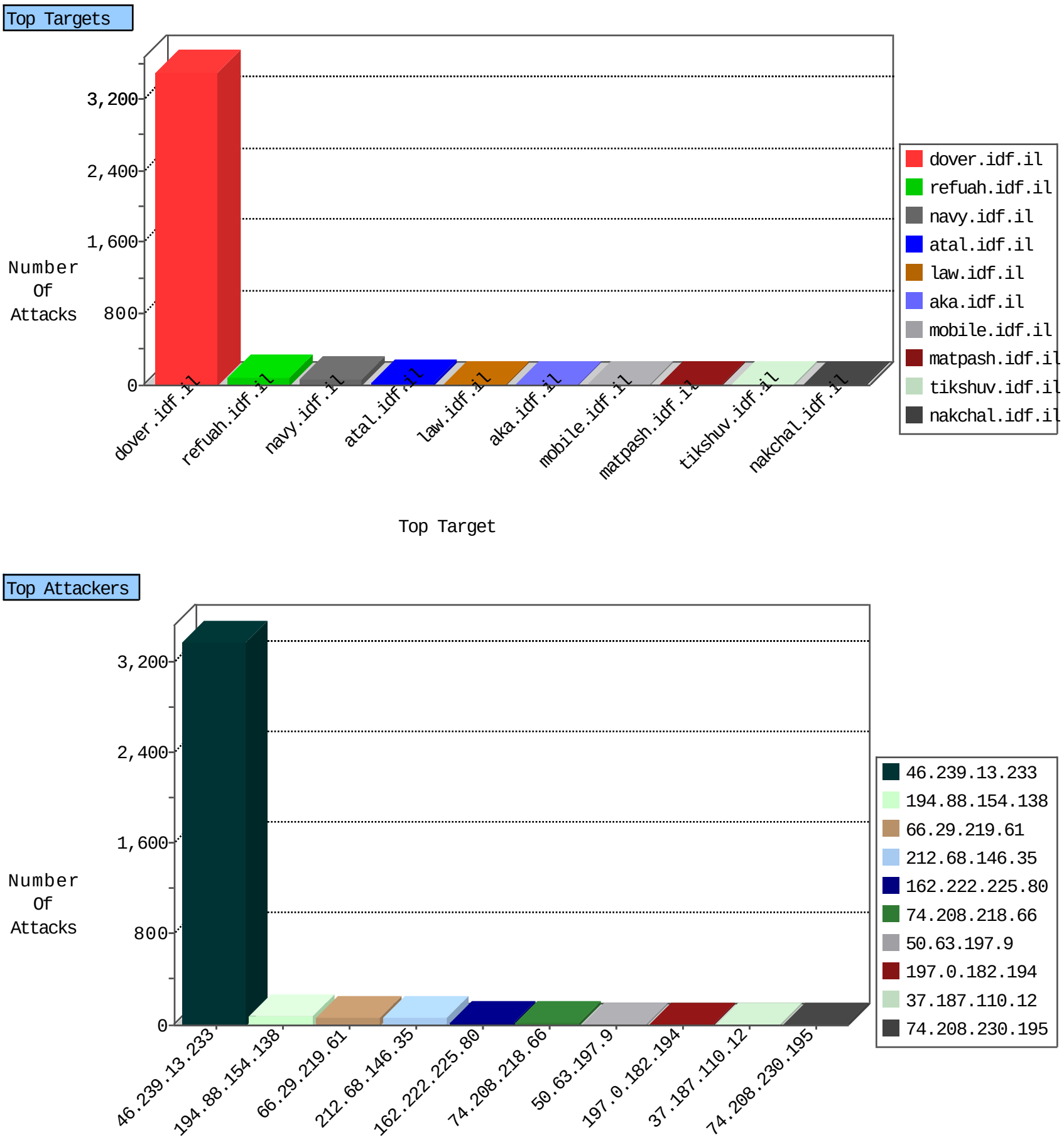
08-29-2016-02:04:05 to 08-29-2016-03:04:05

IDF Under Attack Daily Report



08-29-2016-02:04:05 to 08-29-2016-03:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.239.13.233	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Http	drop	2
82.80.78.2	Israel	147.237.76.86	navy.idf.il	Black List	drop	2
155.94.142.14	United States	147.237.76.42	refuah.idf.il	Black List	drop	1
5.189.136.84	Germany	147.237.76.199	e.nakchal.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.34	yohalan.idf.il	Black List	drop	1

08-29-2016-02:04:05 to 08-29-2016-03:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.68.146.35	Israel	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
194.88.154.138	Poland	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
37.187.110.12	France	147.237.77.216	dover.idf.il	25004: HTTP: WordPress Pingback Redirect Request	Block	7
66.29.219.61	United States	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
212.68.146.35	Israel	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
50.63.197.9	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
194.88.154.138	Poland	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
66.29.219.61	United States	147.237.76.86	navy.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
66.29.219.61	United States	147.237.76.86	navy.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
162.222.225.80	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
51.254.138.58	France	147.237.77.216	dover.idf.il	25004: HTTP: WordPress Pingback Redirect Request	Block	3
37.59.96.212	France	147.237.77.216	dover.idf.il	25004: HTTP: WordPress Pingback Redirect Request	Block	3

08-29-2016-02:04:05 to 08-29-2016-03:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
194.88.154.138	147.237.76.42	Poland	refuah.idf.il	SQL Injection - Select From	59
66.29.219.61	147.237.76.86	United States	navy.idf.il	SQL Injection - Select From	54
212.68.146.35	147.237.77.216	Israel	dover.idf.il	SQL Injection - Select From	54
162.222.225.80	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	15
50.63.197.9	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
163.172.169.150	147.237.76.196	United Kingdom	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
161.18.157.242	147.237.77.216	Colombia	dover.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
124.83.63.189	147.237.77.233	Philippines	atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.232.98.38	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN NMAP -sS window 4096	1
89.147.200.234	147.237.77.121	Azerbaijan	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.169.150	147.237.76.197	United Kingdom	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
159.203.33.10	147.237.76.44	Canada	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
115.126.242.52	147.237.0.33	Korea, Republic of	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.232.98.38	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN NMAP -sS window 3072	1

08-29-2016-02:04:05 to 08-29-2016-03:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.239.13.233	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3374
74.208.218.66	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	18
74.208.230.195	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	6
197.0.182.194	Tunisia	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
109.253.214.119	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
197.0.182.194	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.169.7.223	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	3
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
37.110.70.90	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	2
176.13.8.48	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.226.40.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.13.244.45	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
183.129.160.229	China	147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	1
106.38.241.105	China	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	1
125.77.28.26	China	147.237.0.35	akaws.idf.il	drop		drop	1
183.129.160.229	China	147.237.0.19	madim.atal.idf.il	drop	SAM rule	drop	1
106.38.241.105	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
106.38.241.105	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
212.143.165.117	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.9.243	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
5.22.130.72	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

08-29-2016-02:04:05 to 08-29-2016-03:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.9.243	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
109.253.193.58	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
72.225.173.182	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	3
66.249.64.22	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	3
37.46.41.210	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	3
77.138.66.125	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/sachar/login/	Block	3
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	2
77.122.109.234	Ukraine	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	2
167.220.232.104	Japan	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in URL from 167.220.232.104	Block	2
68.180.228.231	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-11019-en/cogat.aspx.	Block	1
46.19.86.5	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
80.246.130.203	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
157.55.39.97	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
68.180.230.47	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/eng	Block	1
66.102.9.118	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
207.46.13.30	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/faq/faq.aspx	Block	1
84.109.56.206	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
66.249.88.42	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
157.55.39.101	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
207.46.13.64	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mp/	Block	1
95.27.9.231	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.249.88.52	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.46.38.98	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
157.55.39.174	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
108.41.137.241	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
66.249.93.68	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1

08-29-2016-02:04:05 to 08-29-2016-03:04:05