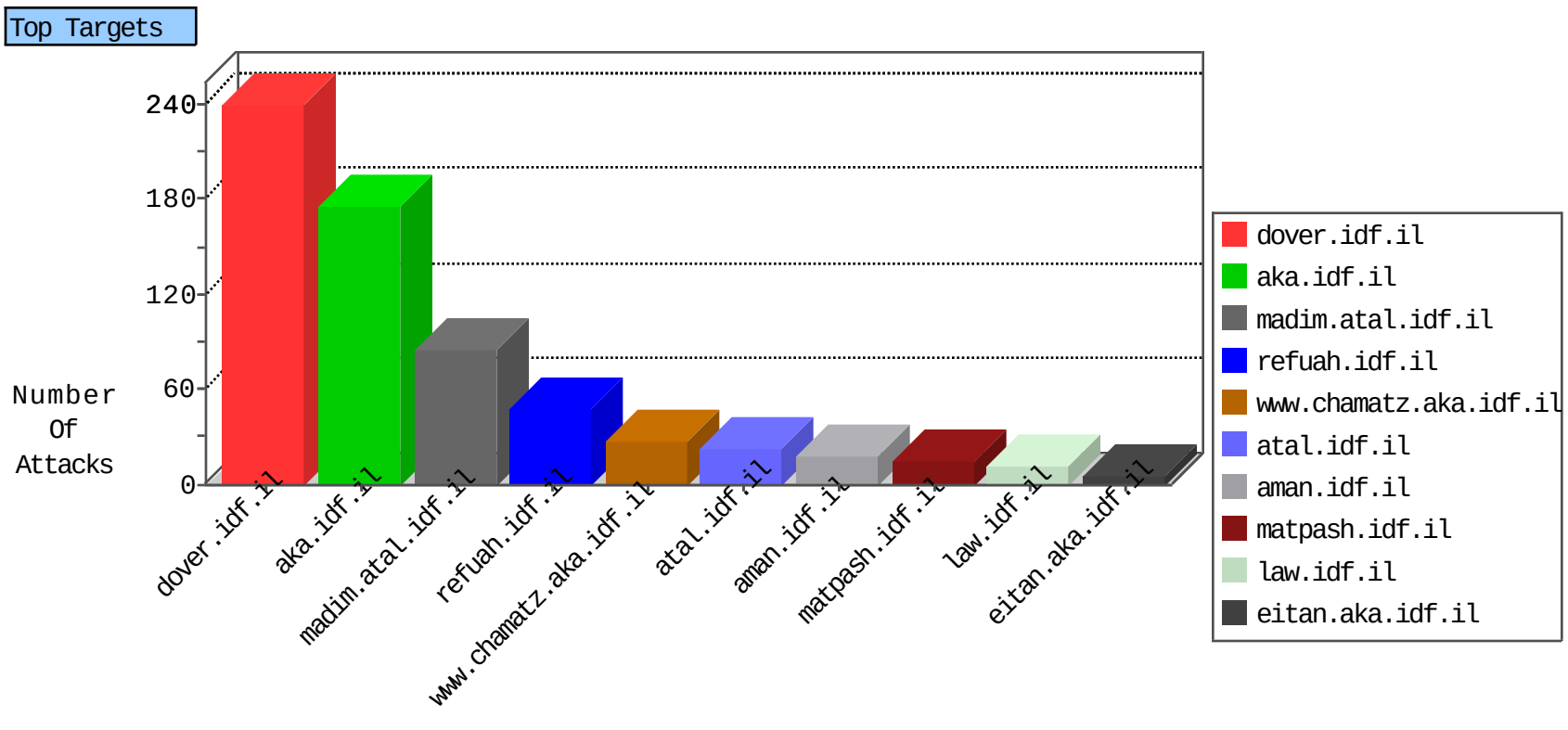
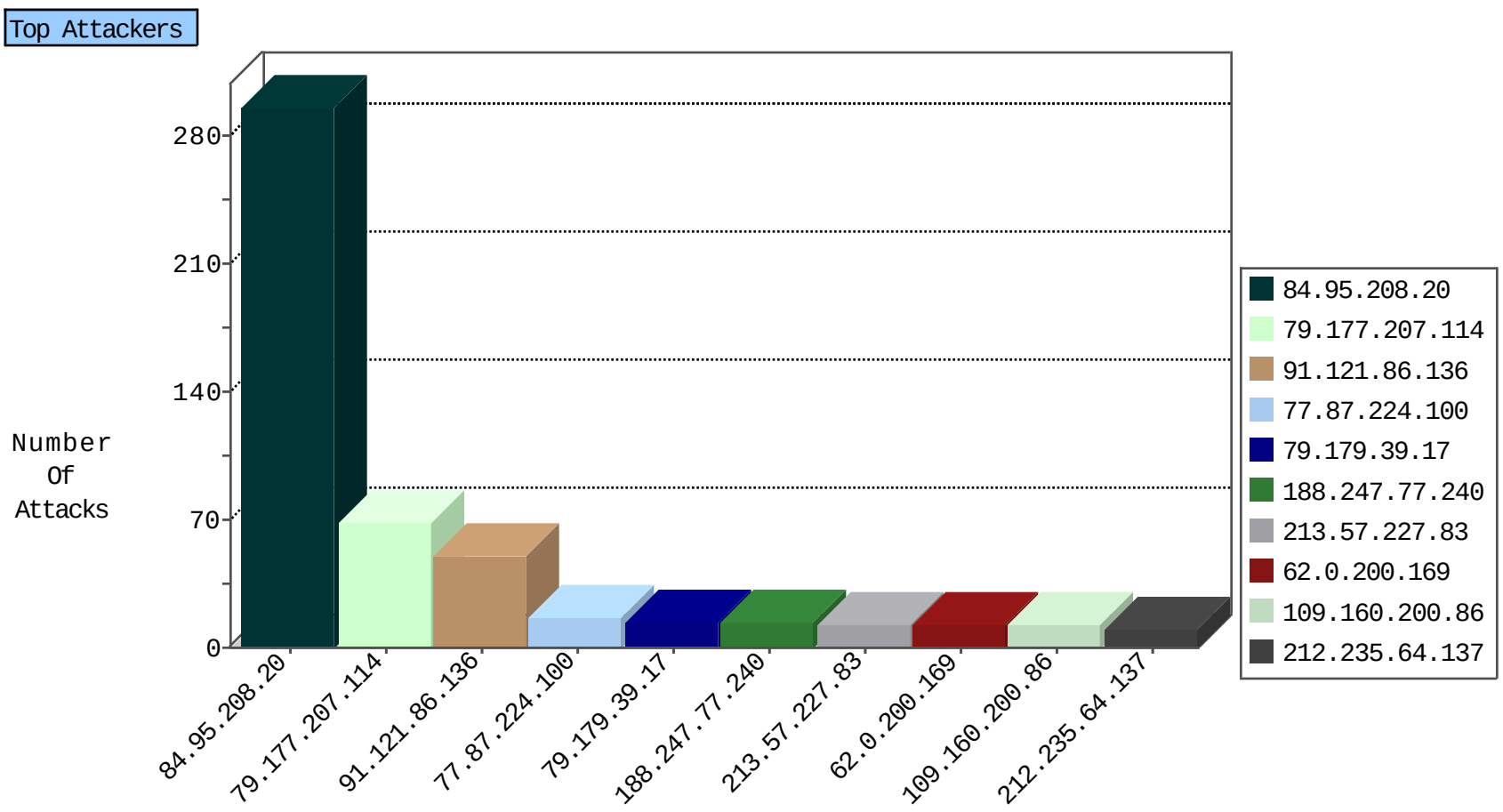
08-18-2016-16:04:05 to 08-18-2016-17:04:05

IDF Under Attack
Daily Report





08-18-2016-16:04:05 to 08-18-2016-17:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.59.59.52	China	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
93.158.200.92	Netherlands	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
27.33.20.47	Australia	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	1
108.233.154.81	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
185.94.111.1	Russian Federation	147.237.76.177	ncore.idf.il	Black List	drop	1
61.139.54.71	China	147.237.77.74	law.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
123.59.59.52	China	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	1
77.87.224.100	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

08-18-2016-16:04:05 to 08-18-2016-17:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.121.86.136	France	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	38
91.121.86.136	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	7
91.121.86.136	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
199.58.86.209	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
91.121.86.136	France	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	2
66.240.219.146	United States	147.237.76.201	e.atal.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
163.172.211.135	United Kingdom	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

08-18-2016-16:04:05 to 08-18-2016-17:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	**Signature**	**Count**

08-18-2016-16:04:05 to 08-18-2016-17:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.87.224.100	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
188.247.77.240	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
62.0.200.169	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
109.160.200.86	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
213.57.227.83	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
66.102.9.21	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	7
212.235.64.137	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	7
66.102.9.111	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	5
109.253.206.32	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
84.95.208.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.67.121.39	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.102.9.101	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	4
66.249.81.182	Europe	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	3
212.235.64.137	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
176.13.11.131	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3
68.180.228.185	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.66.177	United States	147.237.77.216	dover.idf.il	drop		drop	2
69.175.127.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
212.199.218.246	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
66.102.9.31	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
2.53.29.230	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.102.9.91	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	2
2.53.32.141	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
85.130.246.163	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
77.127.79.208	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
49.32.36.187	India	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
66.102.9.20	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
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
104.130.161.143	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
212.143.165.117	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.77.19	law-forum.idf.il	drop	SAM rule	drop	1
216.218.206.106	United States	147.237.0.33	idf.il	drop		drop	1
180.97.106.162	China	147.237.77.235	sviva.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.8.24	e.lifestyle.idf.il	drop	SAM rule	drop	1
107.23.175.47	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	drop	SAM rule	drop	1
109.253.211.153	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
85.130.231.105	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
216.218.206.112	United States	147.237.0.35	akaws.idf.il	drop		drop	1
183.129.160.229	China	147.237.72.14	dover.idf.il(old)	drop	SAM rule	drop	1
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	1
176.13.9.157	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	1
216.243.31.2	United States	147.237.0.35	akaws.idf.il	drop		drop	1
66.249.92.114	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.76.44	e.refuah.idf.il	drop	SAM rule	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	130
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	100
79.177.207.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	68
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	20
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	12
2.53.14.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
79.179.39.17	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 79.179.39.17	Block	8
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	8
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	6
5.28.190.39	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	5
2.53.24.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
213.8.204.74	Israel	147.237.0.34	tikshuv.idf.il	Distributed Suspicious Response Code	Block	4
89.139.51.52	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	4
79.179.39.17	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/עמוד-לא-נמצא	Block	4
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	3
109.253.217.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.102.9.42	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
214.3.138.230	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g51ei5nuhg	Block	2
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
66.102.9.20	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.67.178.63	Israel	147.237.72.156	aman.idf.il	Multiple Double URL Encoding from 109.67.178.63	Block	1
77.125.64.202	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
79.179.39.17	Israel	147.237.76.42	refuah.idf.il	Extremely Long Parameter in www.refua.atal.idf.il %2FwEPDwUKMTU2Nzk2MDgyNw9kFgJmD2QWBAIBD2QWBgICDxYCHgRUZXh0BfgIPGxpbmsgcmVsPSJzdHlsZXNoZWV0IiB0eXBlPS	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.177	Block	1
46.116.93.94	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/4/	Block	1
77.138.173.76	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/giyus/general/	Block	1
66.102.9.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
86.177.176.211	United Kingdom	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
23.20.60.205	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
89.139.232.81	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
64.233.172.161	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/	Block	1
2.53.15.193	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
77.138.217.248	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
109.253.245.110	Israel	147.237.77.243	mobile.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.102.9.85	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
87.69.161.153	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/ru	Block	1
37.26.149.224	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
91.121.86.136	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-17275-he/חיל האוויר תקף שלוש מטרות טרור ברצועה בתגובה לירי הרקטות.aspx	Block	1
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
207.46.13.145	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
66.102.9.105	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/smalim/smalim.aspx	Block	1
87.70.243.157	Israel	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	1
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1