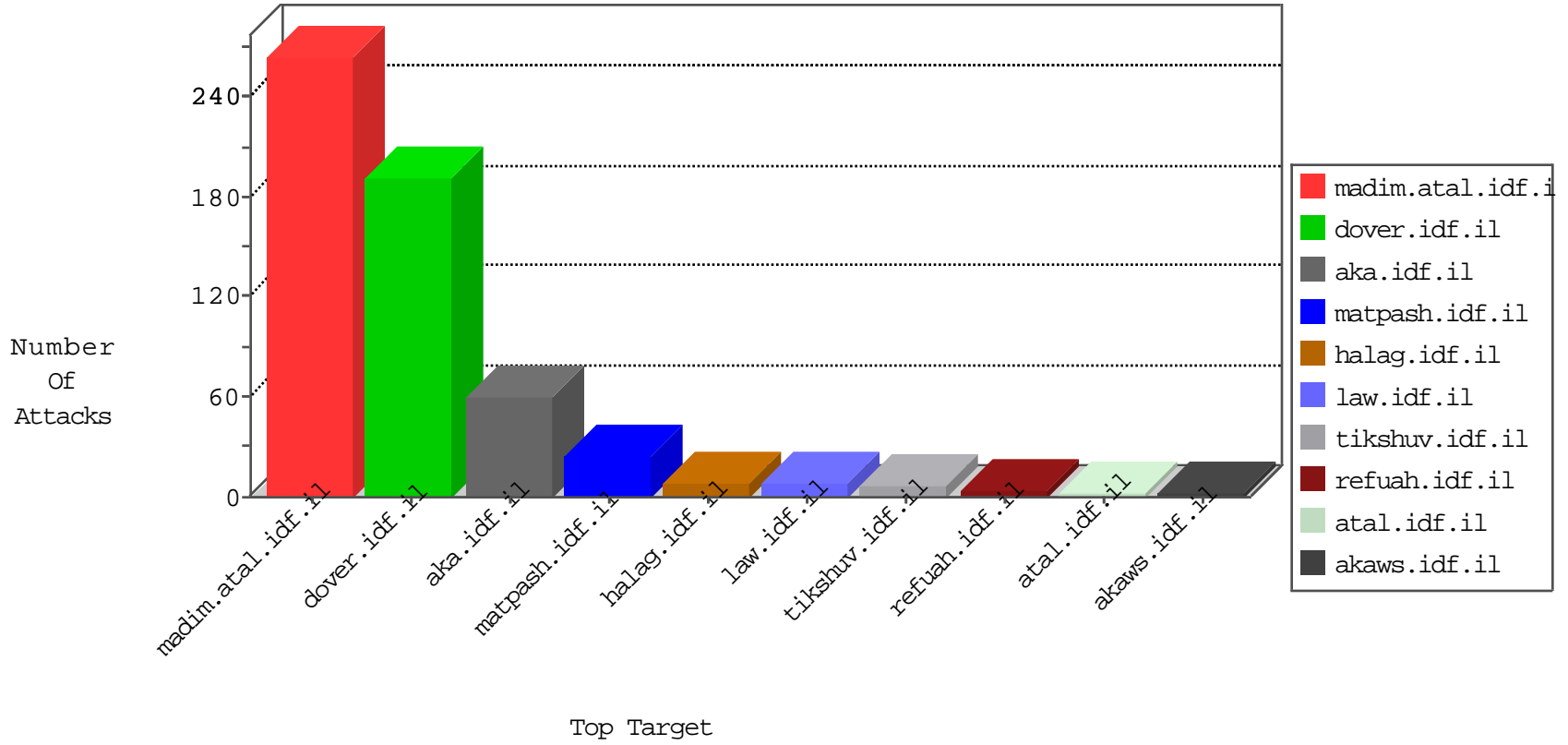


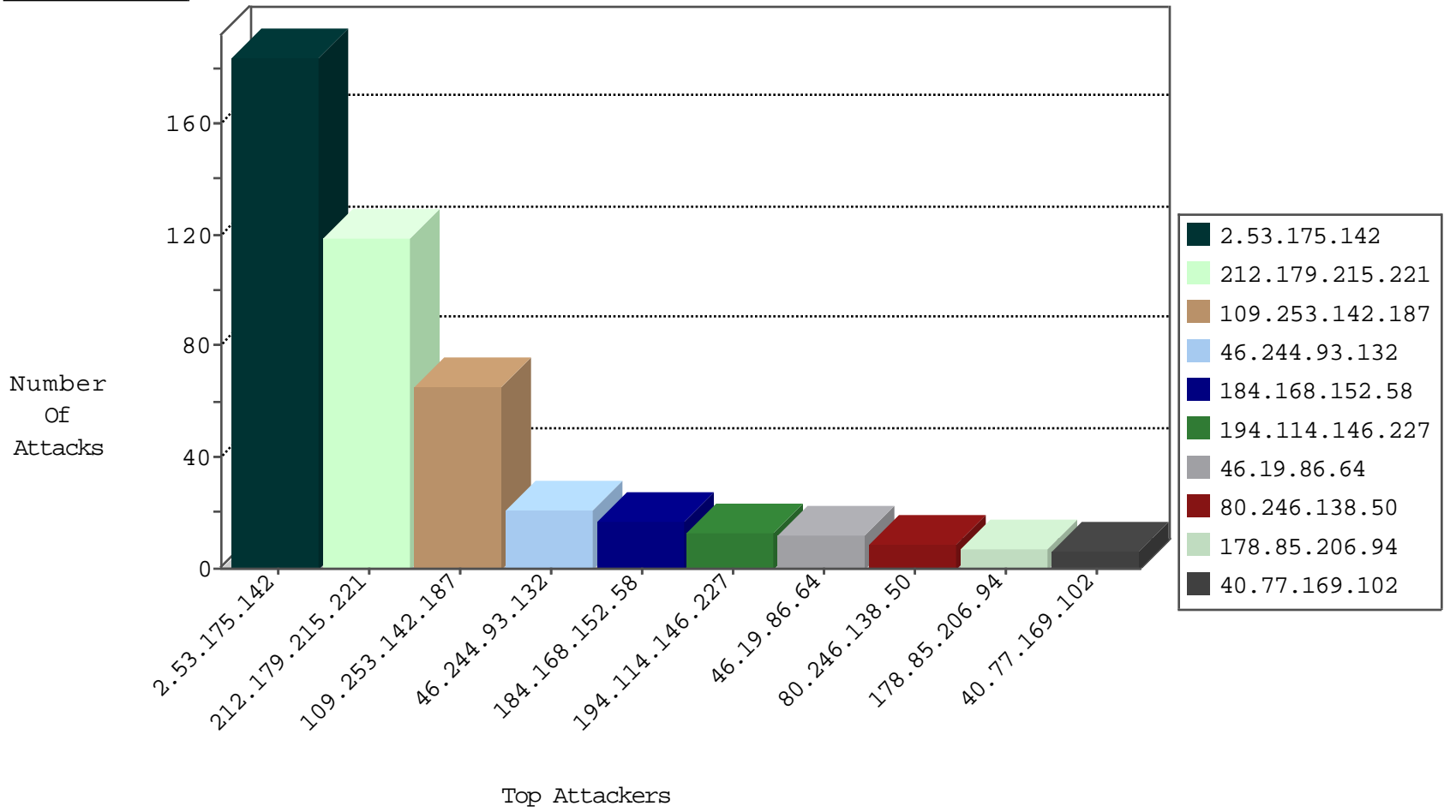
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.147.22	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
46.19.85.196	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
2.53.161.188	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
2.53.163.182	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
104.148.117.90	United States	147.237.76.30	himush.idf.il	Black List	drop	1
80.82.70.230	Netherlands	147.237.76.38	e.e.meitav.idf.i	Black List	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
184.168.152.58	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
138.201.125.143	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	3
64.16.214.100	United States	147.237.77.216	dover.idf.il	C1000003: HTTP: phpMyAdmin access	Permit	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
184.168.152.58	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	11
213.229.77.24	147.237.77.74	United Kingdom	law.idf.il	Tehila - Perl LWP with fake user agent	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.215.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	91
46.244.93.132	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	21
46.19.86.64	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
212.179.215.221	Israel	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	8
178.85.206.94	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
212.179.215.221	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
199.203.179.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.179.215.221	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	4
213.244.65.254	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
176.13.236.85	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.116.34.127	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
109.253.134.67	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
31.13.112.120	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
31.154.80.17	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
40.77.169.102	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
85.130.223.95	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.190	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
212.179.215.221	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.203.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
31.13.100.116	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
92.124.239.7	Russian Federation	147.237.0.35	akaws.idf.il	drop		drop	1
216.243.31.2	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
212.179.71.70	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	1
109.253.222.117	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
31.13.100.117	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
193.95.53.33	Tunisia	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
92.124.239.7	Russian Federation	147.237.76.34	yohalan.idf.il	drop		drop	1
122.172.67.246	India	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
31.13.100.119	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
194.114.146.227	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
31.13.102.108	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
216.243.31.2	United States	147.237.0.33	idf.il	drop		drop	1
109.253.144.210	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
31.13.100.115	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.245.190	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
85.130.223.95	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
31.13.102.127	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
216.243.31.2	United States	147.237.0.35	akaws.idf.il	drop		drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.175.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	184
109.253.142.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	65
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 194.114.146.227	Block	9
80.246.138.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
40.77.169.103	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	5
40.77.169.98	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	5
192.118.10.10	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.118.10.10	Block	5
212.179.215.221	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	4
109.253.137.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
40.77.169.100	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
40.77.169.101	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/0/	Block	3
40.77.169.97	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
109.253.241.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.179.215.221	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	2
192.118.10.10	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/searchback.png	Block	1
40.77.169.99	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
79.176.72.174	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
199.203.127.162	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layout2.css	Block	1
40.77.169.102	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
157.55.39.182	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/default.asp	Block	1
84.109.81.22	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.102.6.25	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
192.198.151.45	Europe	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/exampcert/	Block	1
79.183.39.59	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.150.112.56	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
40.77.169.98	United States	147.237.77.74	law.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
159.220.74.5	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/iturim/asp/displayonesoldier.asp	Block	1
85.250.150.133	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.102.9.43	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/drushim/	Block	1
46.19.86.87	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
212.179.21.194	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatgauntity.aspx	Block	1
169.253.194.1	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
87.71.6.46	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsunemofet.aspx	None	1
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal/izkor/view_img.asp	Block	1
40.77.169.102	United States	147.237.77.74	law.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
2.53.148.79	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
131.130.48.138	Austria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
81.218.56.171	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/shared/hometitleback.gif	Block	1
62.219.147.212	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	1
212.179.71.70	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1250-he/atal.aspx	Block	1
40.77.169.99	United States	147.237.77.176	matpash.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
109.67.26.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
199.30.25.115	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
40.77.169.102	United States	147.237.77.176	matpash.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
144.76.236.183	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
81.218.118.126	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
62.219.147.212	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/261-5815-he/	Block	1