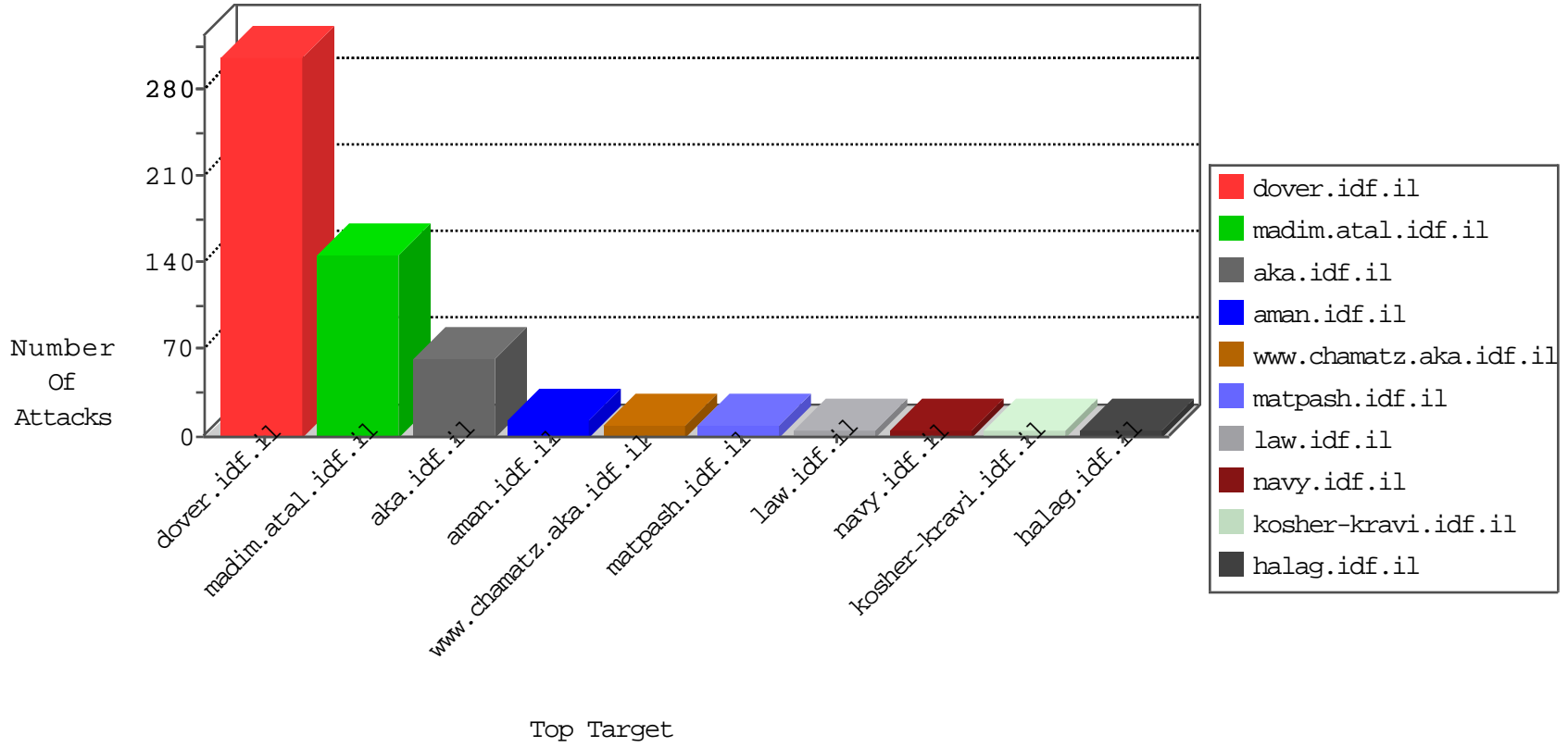


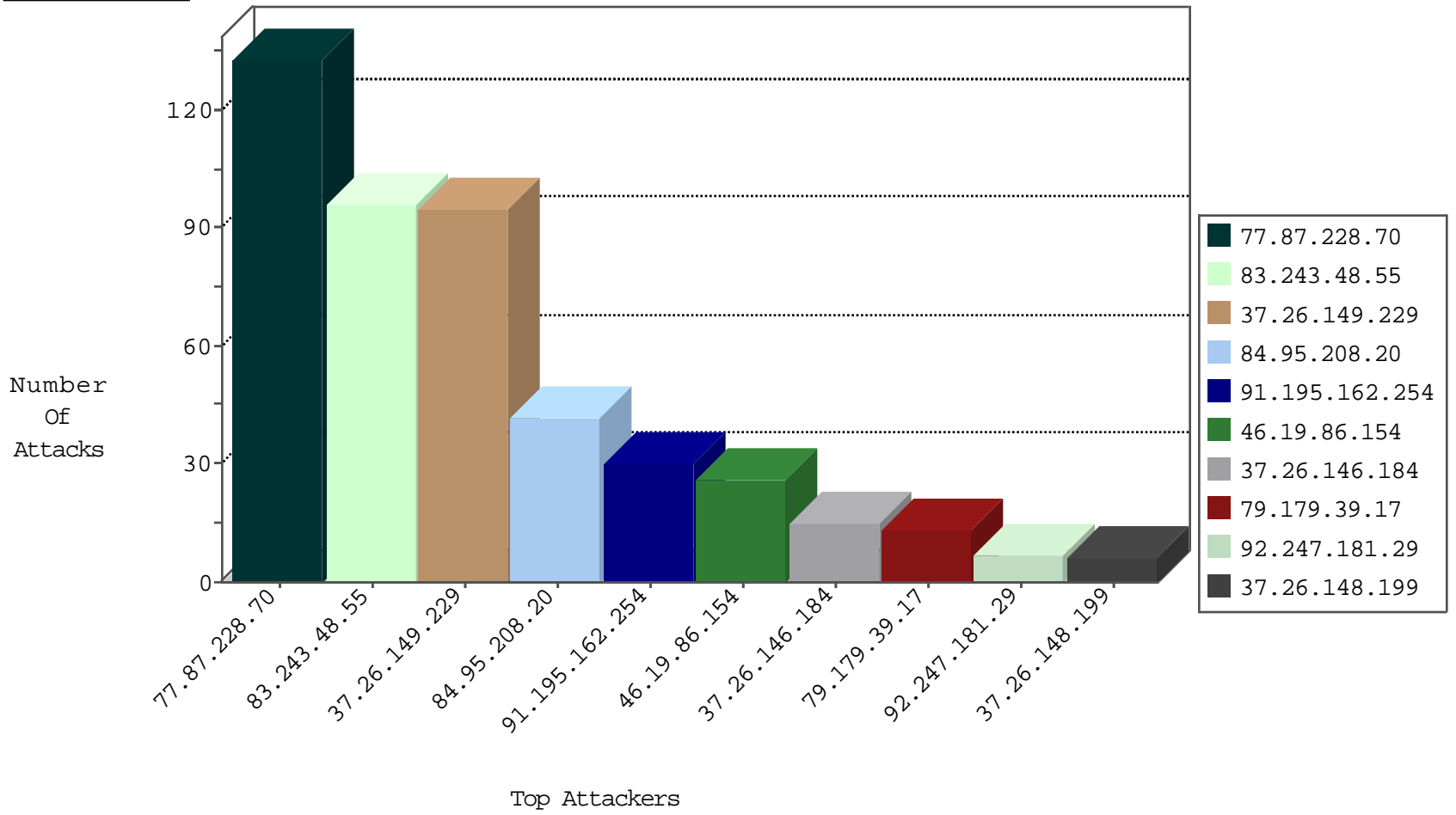
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.148.199	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	18
58.218.204.245	China	147.237.76.177	ncore.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
123.164.227.204	China	147.237.76.44	e.refuah.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
192.99.37.215	Canada	147.237.76.34	yohalan.idf.il	Black List	drop	1
79.179.169.18	Israel	147.237.77.216	dover.idf.il	Black List	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
184.168.46.74	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
------------------	----------------	------------------	------	-----------	-------

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.87.228.70	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	133
83.243.48.55	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	96
91.195.162.254	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	30
92.247.181.29	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
86.104.161.7	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
80.246.133.208	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
37.26.148.199	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
157.55.39.131	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
84.95.208.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
212.117.143.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.253.217.204	Israel	147.237.72.166	aka.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
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.13.11.124	Israel	147.237.72.166	aka.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
177.134.105.235	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.147.174	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
5.22.129.231	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
180.97.106.37	China	147.237.0.17	m.my-kosher-kravi.idf.il	drop	SAM rule	drop	1
197.164.181.144	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
109.253.208.149	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
180.97.106.161	China	147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
77.127.79.208	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
176.13.3.10	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
85.130.190.227	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
64.233.172.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
180.97.106.161	China	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.72.217	e.idf.il	drop	SAM rule	drop	1
109.64.14.243	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.37	United States	147.237.0.200	m4u.idf.il	drop		drop	1
66.249.65.153	Israel	147.237.0.33	idf.il	drop		drop	1
180.97.106.162	China	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	1
212.235.64.137	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.38	United States	147.237.0.200	m4u.idf.il	drop		drop	1
91.113.174.162	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
74.82.47.54	United States	147.237.0.33	idf.il	drop		drop	1
183.129.160.229	China	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.76.86	navy.idf.il	drop	SAM rule	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.149.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	95
46.19.86.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
37.26.146.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	6
176.13.226.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	4
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
46.19.86.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
79.179.39.17	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ - -	Block	3
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
69.118.193.9	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	2
157.55.39.131	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
207.46.13.30	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	2
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	2
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
89.248.140.16	Netherlands	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunselectquestionnaire.aspx	Block	2
109.253.206.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.95.208.20	Israel	147.237.77.234	halag.idf.il	PHP Attempt	Block	1
66.249.76.63	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/piwik.php	Block	1
220.255.183.134	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
203.127.96.220	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
104.128.144.131	Canada	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/redirect.php	Block	1
66.249.65.179	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakchal.idf.il/page.asp	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	PHP Attempt	Block	1
2.55.136.4	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	1
79.179.39.17	Israel	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 79.179.39.17	Block	1
85.65.47.44	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/promotioncube/	Block	1
220.255.219.58	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	PHP Attempt	Block	1
109.67.176.156	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
77.138.217.112	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
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
5.100.86.15	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/rights/asp/info.asp	Block	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal	Block	1
176.13.21.166	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
87.71.36.24	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
66.102.9.19	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
212.179.21.194	Israel	147.237.77.74	law.idf.il	Parameter Type Violation ? in www.law.idf.il/163-7585-he/patzar.aspx	Block	1
77.138.220.97	France	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
109.253.195.116	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.66.183	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1824-22117-he/dover.aspx	Block	1
213.57.143.236	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1