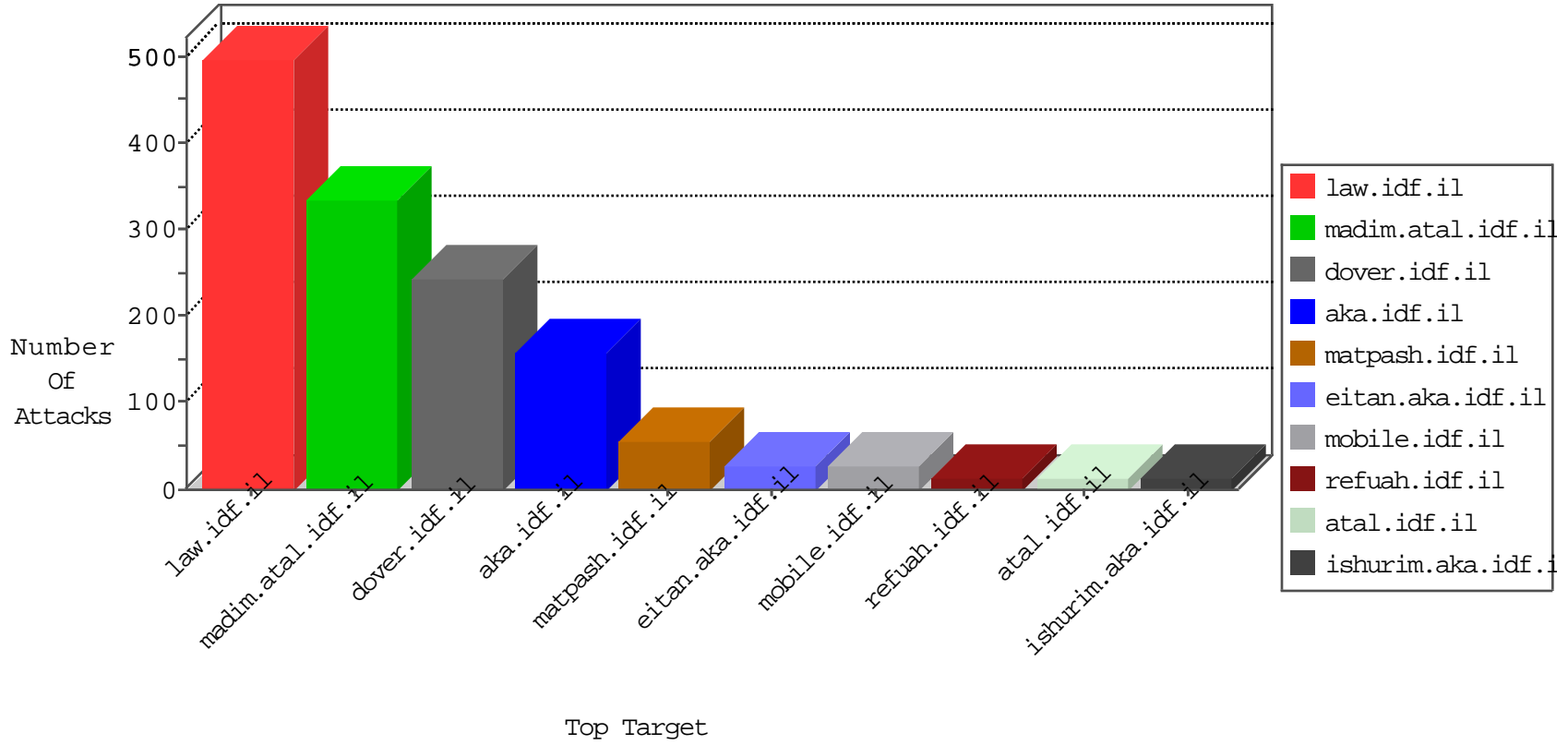


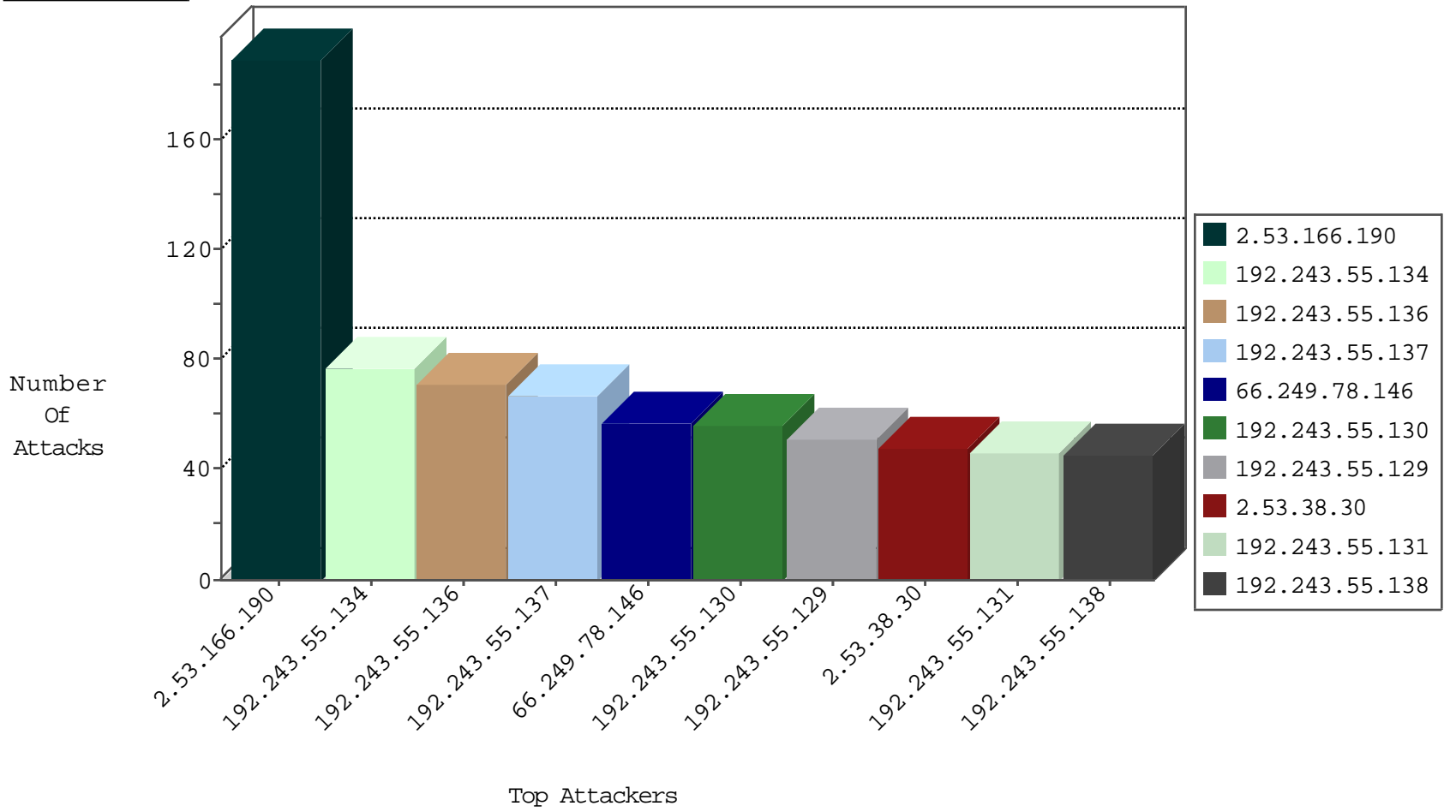
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9978
84.108.43.79	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	5
204.42.253.2	United States	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
82.165.135.208	Germany	147.237.76.200	eitan.aka.idf.il	JIM_Purple_Con_Limit_Http	drop	1
185.94.111.1	Russian Federation	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
204.42.253.2	United States	147.237.76.176	test.ncore.idf.i	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

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

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	57
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	27
46.244.66.58	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	26
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	24
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	20
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	20
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	18
212.143.99.102	Israel	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
192.243.55.134	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
192.243.55.136	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
192.243.55.137	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	12
192.243.55.129	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
85.255.233.136	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
192.243.55.137	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
192.243.55.136	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	10
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
192.243.55.130	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
192.243.55.130	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	9
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
82.213.32.130	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	9
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
192.243.55.131	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
192.243.55.138	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
176.228.28.61	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	7
37.26.146.215	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.135	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.221	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.131	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.132	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.166.190	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	189
2.53.38.30	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	46
185.32.179.114	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	41
46.19.86.238	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	7
2.53.1.178	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
109.253.226.45	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
109.253.226.52	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.53.29.208	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
178.137.93.24	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 178.137.93.24	Block	3
109.253.226.49	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.53.41.162	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.226.29	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.226.54	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.53.29.208	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
79.181.245.89	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	2
80.246.136.178	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	2
157.55.39.37	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
95.158.243.78	Russian Federation	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/404.aspx'steam	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.234	Block	1
207.46.13.87	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/registrationwizard/register.aspx	Block	1
5.28.135.147	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
178.137.93.24	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
187.44.148.42	Brazil	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/wp-login.php	Block	1
46.19.86.60	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/general/mobile	Block	1
157.55.39.37	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-16782-en/dover.a sp< />spx	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2027-he/cogat.aspx	Block	1
207.46.13.98	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/news/news.in.aspx	Block	1
5.28.135.147	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
180.76.15.143	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9059-he/refuah.aspx	Block	1
109.253.226.53	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/buttonback.png	Block	1
192.243.55.130	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/shared/usercontrols/lobbyinfocenteritem	Block	1
2.53.150.171	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
164.132.161.61	Italy	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
109.253.226.43	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
74.82.47.4	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
207.46.13.143	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
185.3.147.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/contactus/mobile	Block	1
40.77.167.33	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
89.139.227.190	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 89.139.227.190	Block	1
195.191.52.10	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/text.css	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/edim/yoman/yoman.asp	Block	1
178.137.93.24	Ukraine	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
208.115.111.72	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/	Block	1
46.19.85.105	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	1
151.80.31.168	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/yohalan/main1218.html	Block	1
2.53.30.164	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
89.139.227.190	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	1
195.191.52.10	Israel	147.237.76.42	refuah.idf.il	Suspicious Response Code	Block	1