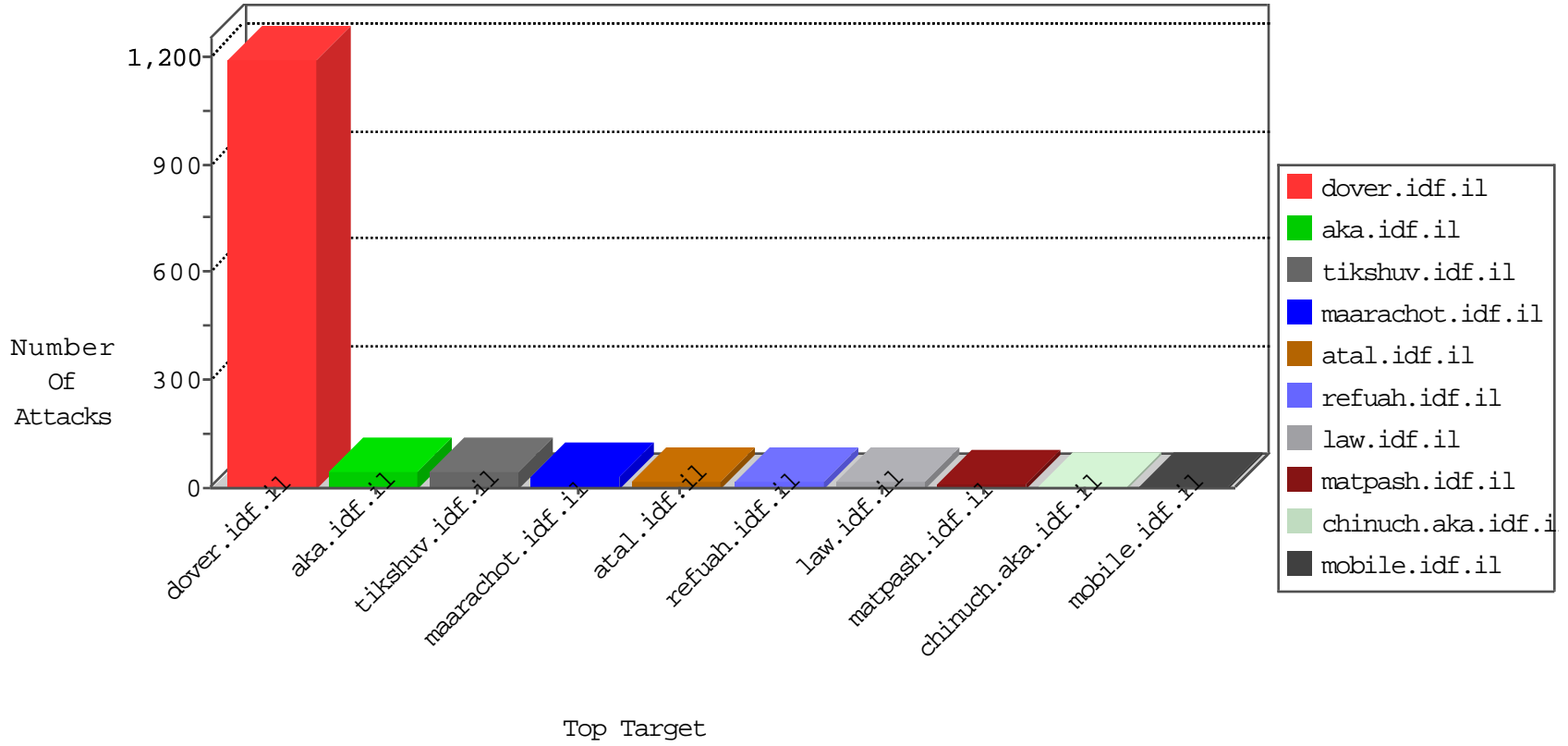


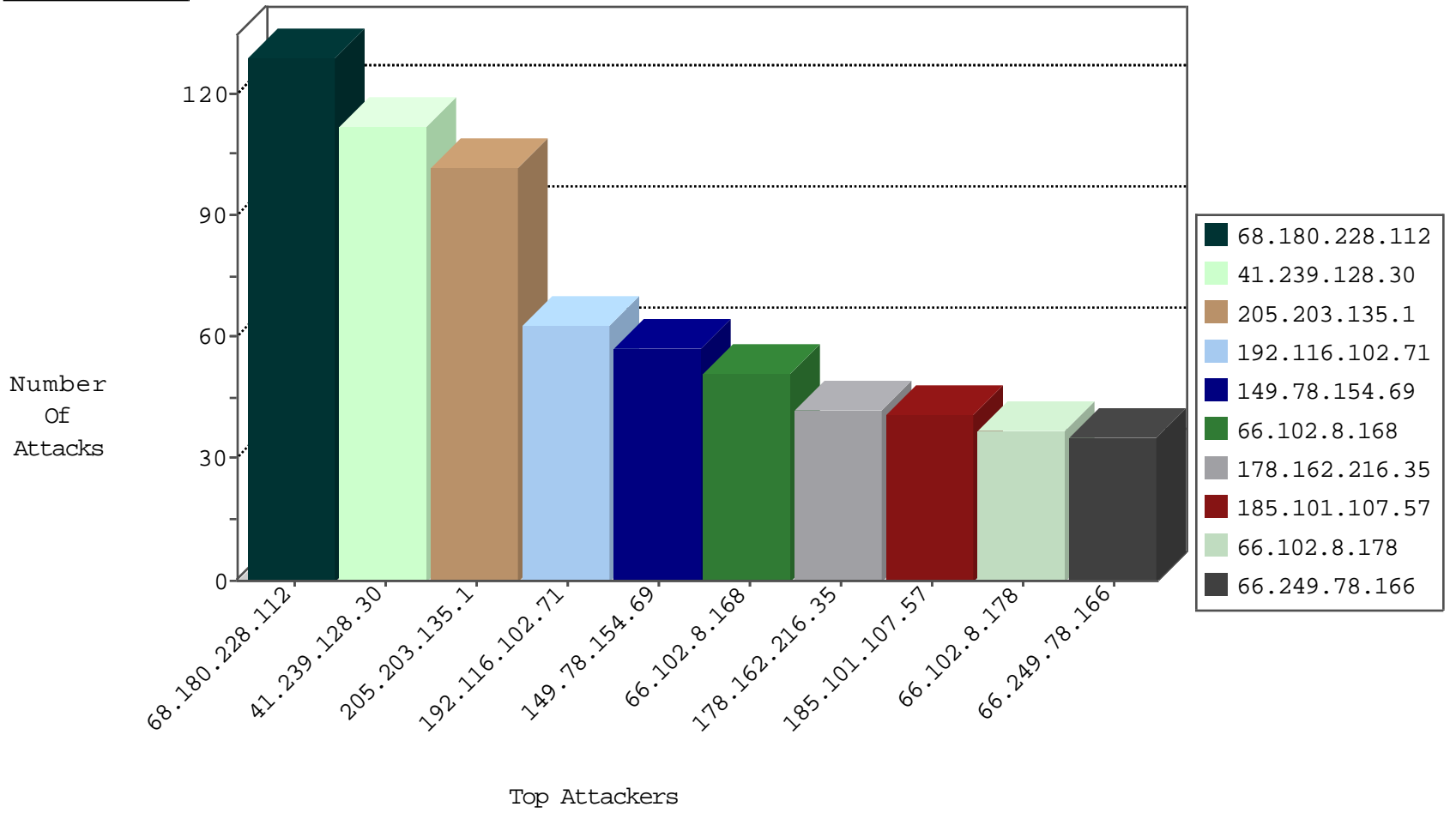
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
96.224.6.115	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
45.63.1.137		147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
81.27.0.0	Sweden	147.237.76.200	eitan.aka.idf.il	Invalid L4 Header Length	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.19.29.90	Turkey	147.237.76.86	navy.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	1
89.19.29.90	Turkey	147.237.76.86	navy.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

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
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	102
41.239.128.30	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
192.116.102.71	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
66.102.8.168	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
185.101.107.57		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	34
66.102.8.178	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
85.114.98.0	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
96.224.6.115	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
40.77.167.35	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
131.253.25.184	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
24.76.249.74	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
79.180.4.188	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
100.100.112.77		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.102.8.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
64.233.172.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
95.86.83.202	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
85.128.142.57	Poland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
73.24.182.255	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
103.229.126.72	Taiwan	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
103.229.126.72	Taiwan	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	7
66.249.88.91	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.140.188.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.88.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
213.57.194.37	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.64.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
69.145.170.136	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	drop	First packet isn't SYN	drop	5
66.102.8.173	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
66.102.8.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
151.80.31.115	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
207.46.13.178	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
77.127.56.21	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
93.157.82.130	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
52.23.156.32	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.65.185.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.108.68.248	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
40.77.167.33	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1379-he/dover.aspx	Block	84
178.162.216.35	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	42
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
41.239.128.30	Egypt	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.239.128.30	Block	28
188.143.232.10	Russian Federation	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 188.143.232.10	Block	14
199.59.148.211	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/8/size220x0/17418.jpg	Block	14
31.193.51.80	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
188.143.232.10	Russian Federation	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/900-en/	Block	14
207.46.13.134	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	14
176.10.104.240	Switzerland	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	14
188.165.15.205	France	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/163-5843-he/patzar.aspx	Block	14
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	14
212.199.136.107	Israel	147.237.0.34	tikshuv.idf.il	Parameter Type Violation FolderId in www.tikshuv.idf.il/modules/forums/forum.aspx	Block	14
66.249.67.134	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on 147.237.77.170/robots.txt	Block	14
199.16.156.124	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/9/size220x0/17429.jpg	Block	14
152.115.70.227	Denmark	147.237.72.166	aka.idf.il	MSSQL Data Retrieval with Implicit Conversion Errors	None	14
184.105.139.67	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	14
66.249.67.143	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	14
199.59.148.209	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/9/size220x0/17429.jpg	Block	14
152.115.70.227	Denmark	147.237.72.166	aka.idf.il	Multiple signatures from 152.115.70.227	Block	14
157.55.39.200	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	11