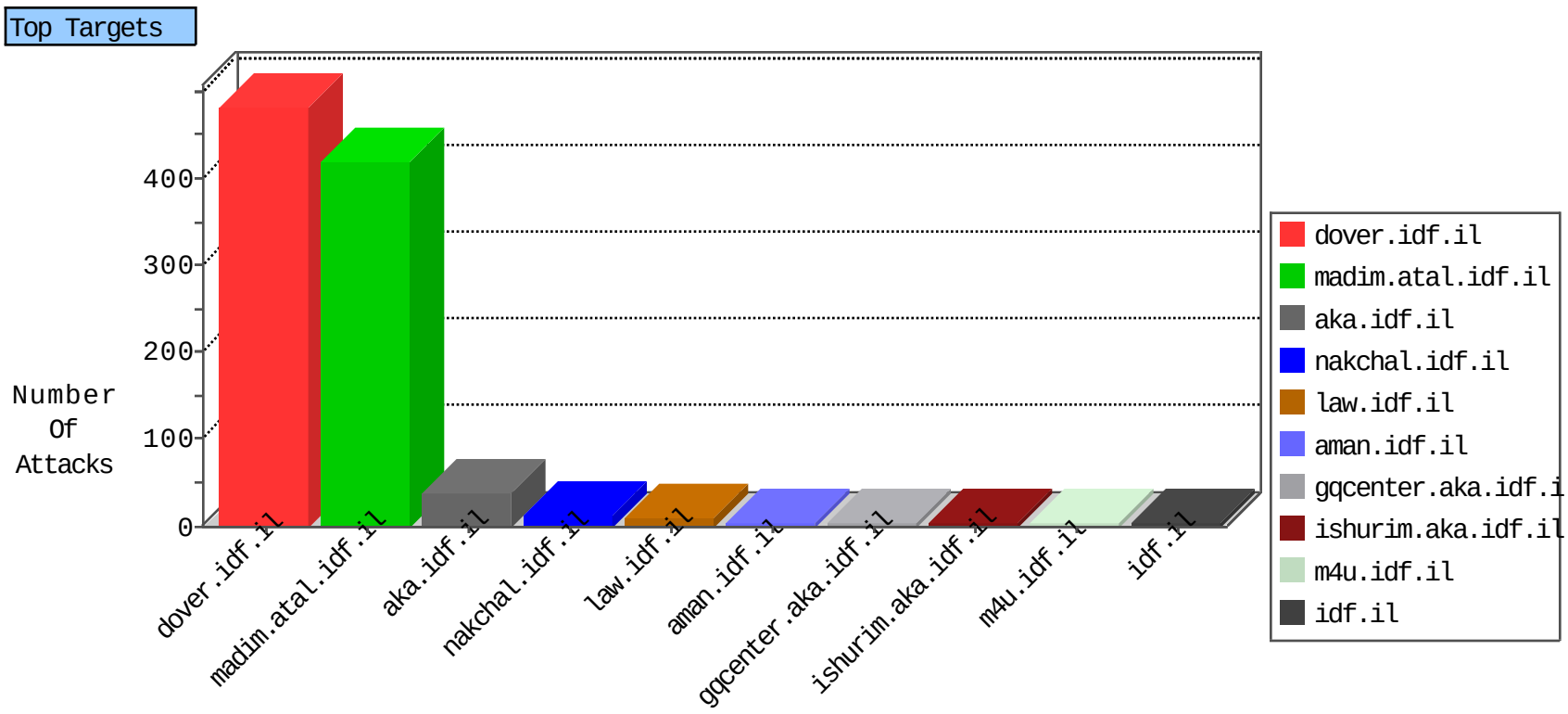
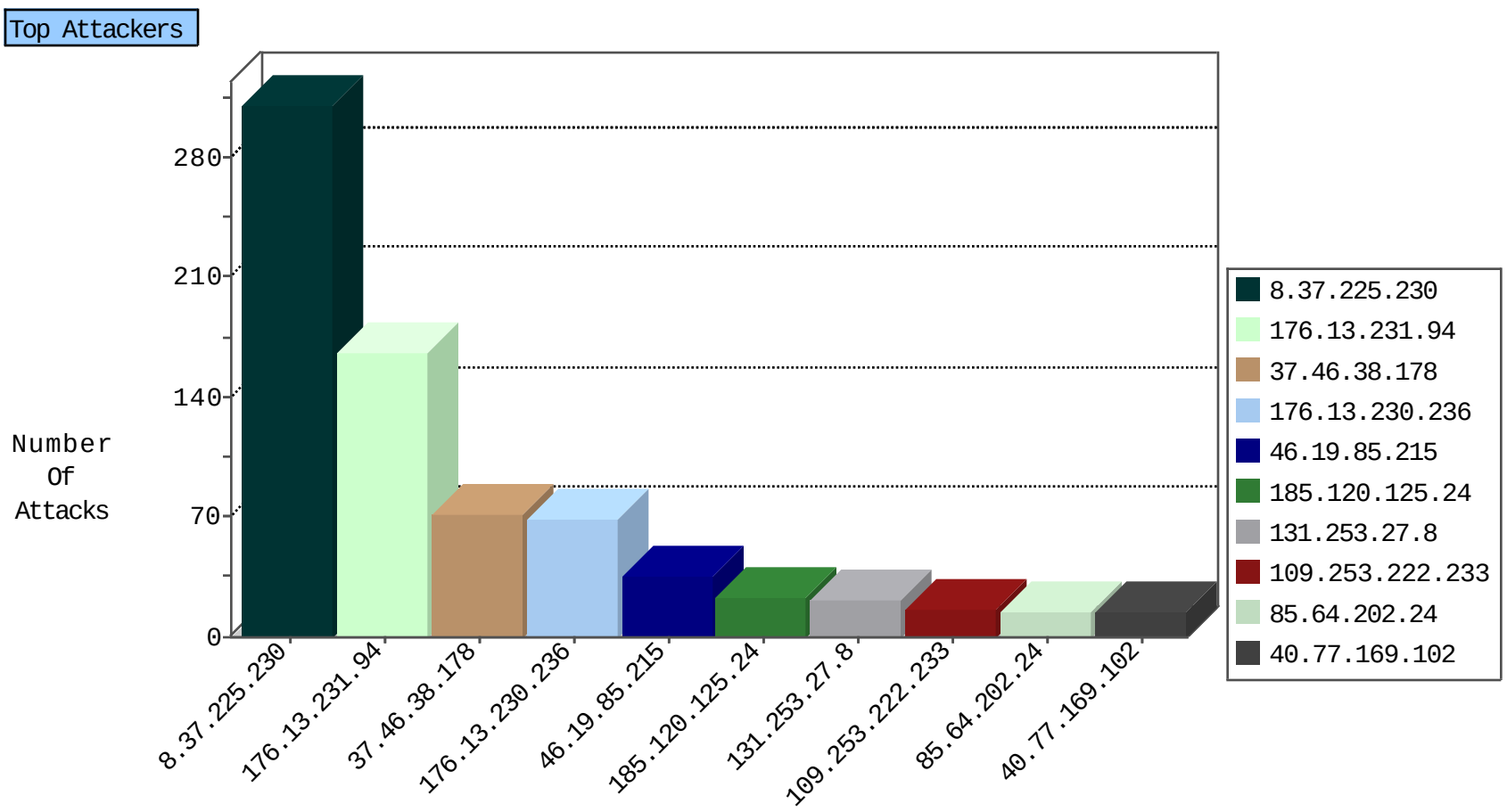
08-29-2016-14:04:08 to 08-29-2016-15:04:08

IDF Under Attack
Daily Report



Top Target



Top Attackers

08-29-2016-14:04:08 to 08-29-2016-15:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.64.202.24	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
8.37.225.230	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
8.37.225.230	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
60.54.75.237	Malaysia	147.237.76.44	e.refuah.idf.il	Black List	drop	2
176.13.231.94	Israel	147.237.0.19	madim.atal.idf.il	DOSS-SSL-ClearText	drop	1
198.48.92.104	United States	147.237.76.30	himush.idf.il	Black List	drop	1
94.102.49.193	Netherlands	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
209.126.136.2	United States	147.237.76.30	himush.idf.il	Black List	drop	1
46.19.86.0	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
95.35.213.133	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
209.126.136.2	United States	147.237.76.202	e.halag.idf.il	Black List	drop	1

08-29-2016-14:04:08 to 08-29-2016-15:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

08-29-2016-14:04:08 to 08-29-2016-15:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
147.235.185.74	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.127.26.247	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
116.12.175.233	147.237.0.15	Singapore	kosher-kravi.idf.i	ET SCAN NMAP -sS window 3072	1
77.124.19.3	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.135.125	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.8	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.186.94.124	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.55.174.179	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.130.223.241	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.53.63.68	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.229.25.132	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
83.130.251.148	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.143.138.22	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.133.241	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
178.220.165.231	147.237.76.198		e.yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
79.178.222.71	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
132.74.209.153	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.124.50.138	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
116.12.175.233	147.237.0.15	Singapore	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
46.19.86.211	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.226.44.128	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.255.90.133	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
109.109.43.232	147.237.0.34	Iran, Islamic Republic of	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
2.53.150.11	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.147.140	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.22.120	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.94.194.70	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.203.37	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.168.13	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.203.83.226	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.179.199.87	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

08-29-2016-14:04:08 to 08-29-2016-15:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
8.37.225.230	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	306
40.77.169.102	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	14
95.35.213.133	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
84.149.194.158	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
193.103.207.10	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.13.13.155	Israel	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	5
62.219.227.25	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
85.130.187.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.117.215.46	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
109.253.145.21	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
80.178.222.233	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
192.169.7.223	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	3
31.168.162.158	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
84.109.1.80	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.253.145.21	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	3
93.84.230.165	Belarus	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
157.55.39.201	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
85.64.202.24	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
68.180.230.47	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
106.38.241.105	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
80.179.41.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
212.143.135.92	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
217.194.197.80	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
80.246.133.248	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
93.63.226.141	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
79.177.125.14	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
37.26.148.252	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
216.243.31.2	United States	147.237.0.200	m4u.idf.il	drop		drop	1
176.13.236.3	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
5.29.38.52	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.113	United States	147.237.0.200	m4u.idf.il	drop		drop	1
176.13.2.163	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
109.253.131.143	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.236.249	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.114	United States	147.237.0.200	m4u.idf.il	drop		drop	1
106.38.241.105	China	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	1
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
46.19.86.225	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	1
176.13.3.95	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
109.253.143.76	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	1
141.212.122.122	United States	147.237.0.33	idf.il	drop		drop	1
106.38.241.105	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
212.199.75.26	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.123	United States	147.237.0.33	idf.il	drop		drop	1
106.38.241.105	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
216.243.31.2	United States	147.237.0.33	idf.il	drop		drop	1
176.13.230.2	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.231.94	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	165
37.46.38.178	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	71
176.13.230.236	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	67
46.19.85.215	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	35
185.120.125.24	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	23
131.253.27.8	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	22
109.253.222.233	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	16
91.199.73.194	Turkey	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	10
138.134.102.16	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	9
2.53.21.130	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
176.13.244.228	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
46.19.86.89	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
195.160.242.40	Israel	147.237.77.74	law.idf.il	Distributed Unauthorized HTTP Method	Block	4
176.13.19.210	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.55.52.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.247.160	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.148.238	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
91.199.73.196	Turkey	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
2.53.190.67	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
145.255.16.86	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	2
37.26.148.208	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
95.35.131.63	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/geneal.aspx	Block	2
62.219.147.212	Israel	147.237.77.74	law.idf.il	Distributed Unauthorized HTTP Method	Block	2
176.13.230.236	Israel	147.237.0.19	madim.atal.idf.i	Untraceable SSL Sessions: Open Mode	None	2
91.199.73.195	Turkey	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	2
62.219.147.212	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 62.219.147.212	Block	2
212.179.21.194	Israel	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1065-he/dover.aspx parameter SearchText	Block	2
138.134.102.16	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 138.134.102.16	Block	2
109.253.195.181	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
40.77.167.29	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/3/	Block	1
87.71.47.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.235.124.56	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/pniotfindanswer.aspxש'	Block	1
62.0.30.109	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
195.160.242.40	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
77.138.34.98	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
41.187.94.250	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
5.29.221.83	Israel	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1065-he/dover.aspx parameter SearchText	Block	1
213.57.59.18	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
148.251.2.180	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
2.53.23.242	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
101.178.206.92	Australia	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to 147.237.76.200/jetspeed/	Block	1
199.30.24.41	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.177.164.172	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
31.13.113.175	Ireland	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/pniotfindanswer.aspxש'	Block	1
157.55.39.97	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
37.26.149.207	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
2.53.33.135	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
109.66.130.226	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
84.108.249.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1