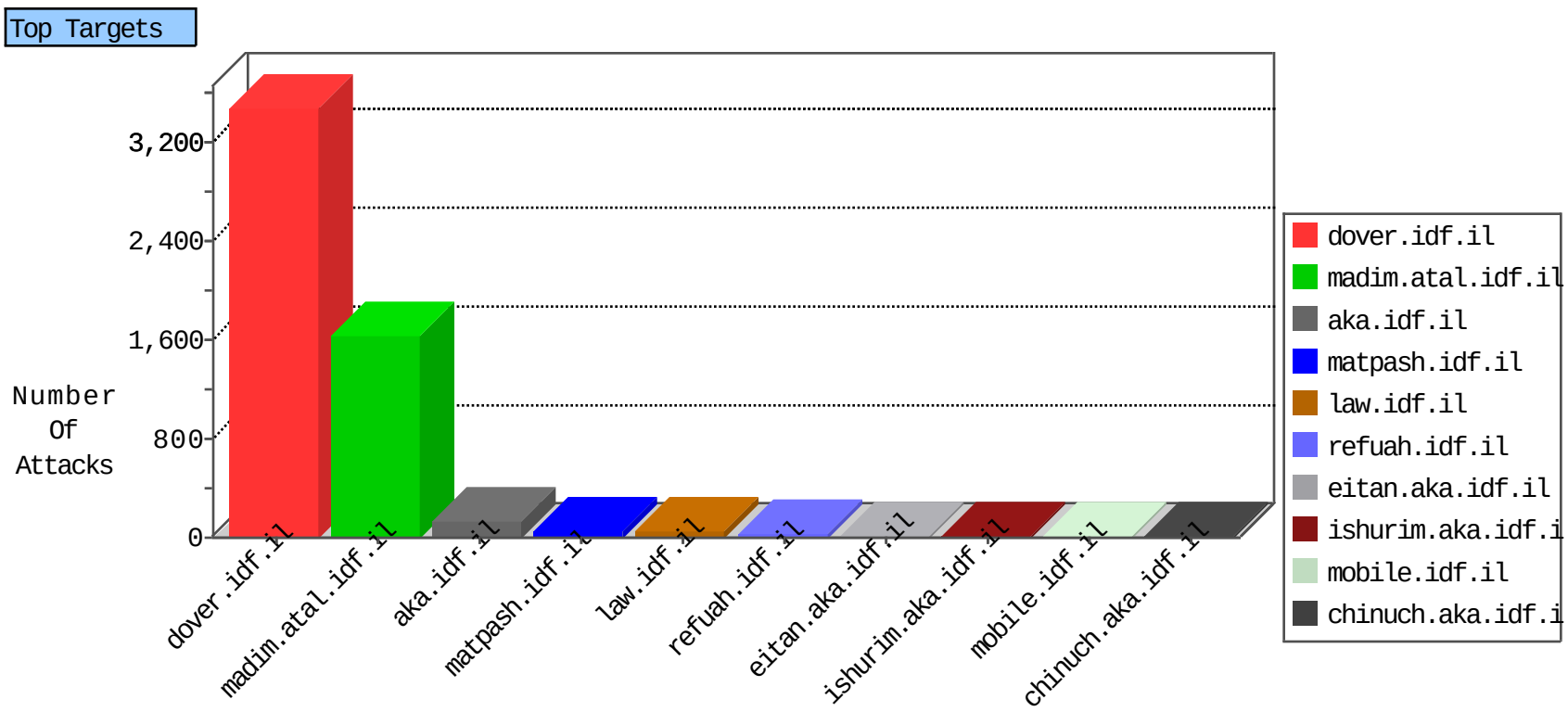
11-08-2015-06:04:02 to 11-08-2015-07:04:02

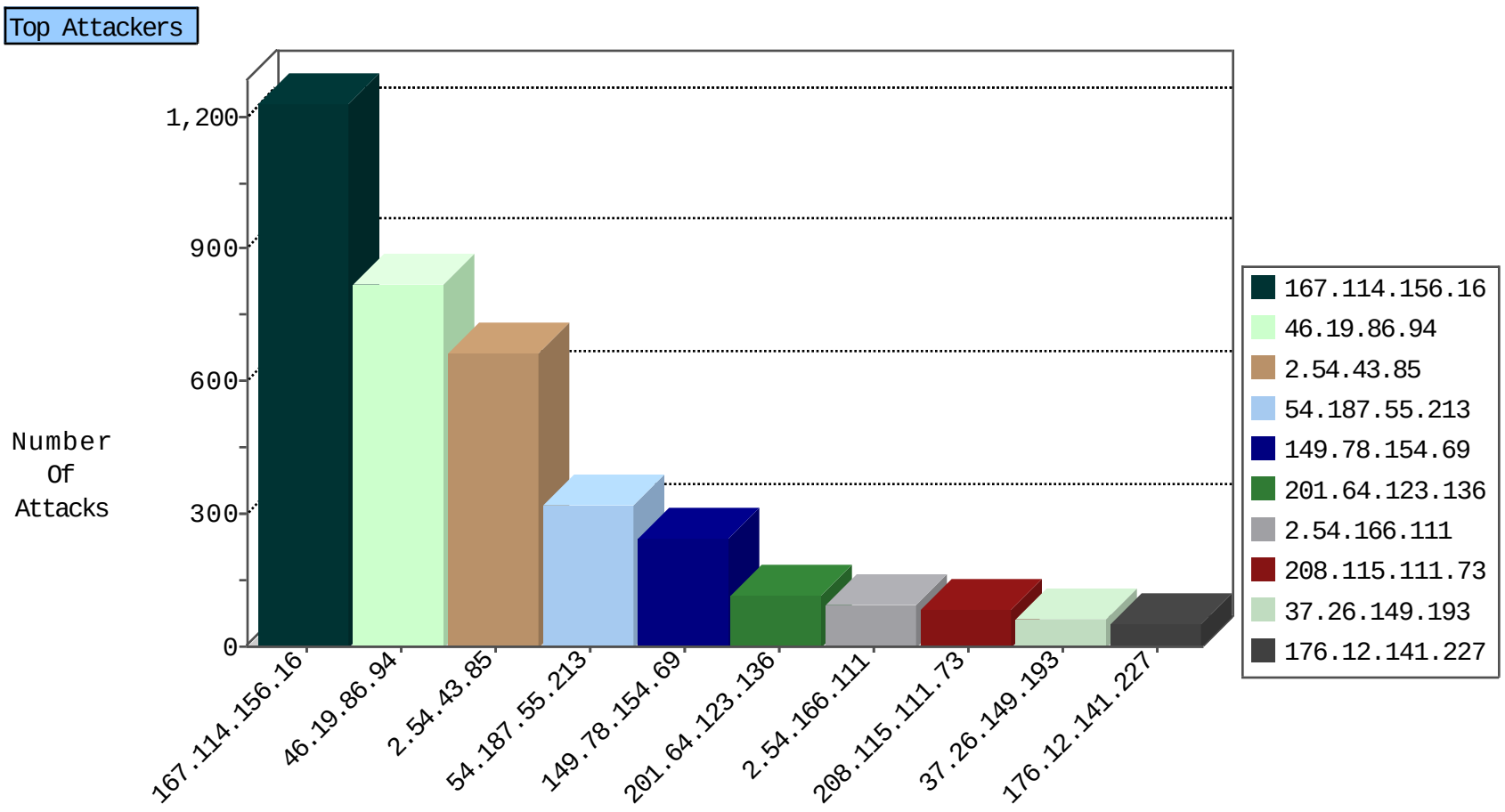
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

11-08-2015-06:04:02 to 11-08-2015-07:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.64.186	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	19303
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	14058
54.244.22.103	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4638
54.187.55.213	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4579
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2297
66.249.67.122	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	373
2.52.171.99	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
46.120.79.166	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
79.181.217.103	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
166.173.249.126	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
54.244.22.103	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
66.249.67.13	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2
46.19.85.73	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
104.192.0.20	United States	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
167.114.82.227	Canada	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
71.6.165.200	United States	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
104.192.0.20	United States	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
5.22.134.111	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
79.179.197.15	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
146.185.239.100	Russian Federation	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	drop	1

11-08-2015-06:04:02 to 11-08-2015-07:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-08-2015-06:04:02 to 11-08-2015-07:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.73.220	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	50
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	9
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.93.199	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
193.107.16.206	147.237.77.233	Russian Federation	atal.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
193.107.16.206	147.237.77.233	Russian Federation	atal.idf.il	ET SCAN NMAP -sS window 1024	1

11-08-2015-06:04:02 to 11-08-2015-07:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	316
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	243
201.64.123.136	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	114
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
176.12.141.227	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
192.0.81.55	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
80.246.130.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
89.139.190.155	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
37.187.157.108	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
70.193.72.227	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
146.135.20.171	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
107.77.90.87	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
73.231.83.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
157.55.39.31	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
66.249.65.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
66.249.65.231	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
107.223.140.164	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
46.19.86.73	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
46.121.140.179	Israel	147.237.76.42	refuah.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
97.93.115.135	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
54.244.22.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
66.102.7.226	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
157.55.39.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
157.55.39.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
79.181.217.103	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
66.102.7.233	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
192.0.81.17	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
66.102.7.240	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
107.170.61.36	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.102.8.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.103.115	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
50.18.94.121	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
5.22.134.111	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
104.189.90.191	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
204.236.155.84	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
157.55.39.175	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.43.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	435
46.19.86.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	358
46.19.86.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	244
46.19.86.94	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.94	Block	142
2.54.43.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
2.54.166.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	94
2.54.43.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	87
46.19.86.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	75
37.26.149.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	60
2.54.43.85	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 2.54.43.85	Block	40
37.142.102.216	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
66.33.204.137	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.33.204.137	Block	5
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
84.95.247.58	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/giyus/login/	Block	2
54.244.22.103	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
199.16.156.125	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/7/size220x0/17487.jpg	Block	1
5.175.26.46	Germany	147.237.76.31	nakchal.idf.il	Distributed Suspicious Response Code	Block	1
98.7.109.156	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
62.210.88.201	France	147.237.77.74	law.idf.il	Unauthorized URL Access to 51.254.206.142/httptest.php	Block	1
199.59.148.209	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/9/size220x0/17479.jpg	Block	1
68.180.228.175	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/163-7183-en/patzaraspx	Block	1
66.249.64.56	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8688-he/refuah.aspx	Block	1
46.19.86.94	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
5.175.26.46	Germany	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
98.7.109.156	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
64.79.85.205	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
206.253.226.23	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
79.182.192.35	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en	Block	1
66.249.64.137	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
157.55.39.189	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
5.175.26.46	Germany	147.237.72.166	aka.idf.il	Unknown Parameter amp;docId in www.aka.idf.il/giyus/forms/	None	1
66.249.67.250	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
64.79.85.205	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;docId in aka.idf.il/giyus/forms/	None	1
208.115.111.73	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/templates/shared/usercontrols/lobbyinfocenteritem/	Block	1
2.54.43.85	Israel	147.237.0.19	madim.atal.idf.il	Too Many 403: Response Code per Session	Block	1
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/yoman.asp	Block	1
46.121.140.179	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/7/size220x0/17487.jpg	Block	1
5.175.26.46	Germany	147.237.72.166	aka.idf.il	Unknown Parameter amp;docId in www.aka.idf.il/giyus/login/	None	1
68.180.228.109	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/shared/usercontrols/headerupper/	Block	1
64.79.85.205	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;docId in aka.idf.il/giyus/login/	None	1
216.218.206.66	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
84.95.247.58	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp in www.aka.idf.il/giyus/login/	None	1
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1