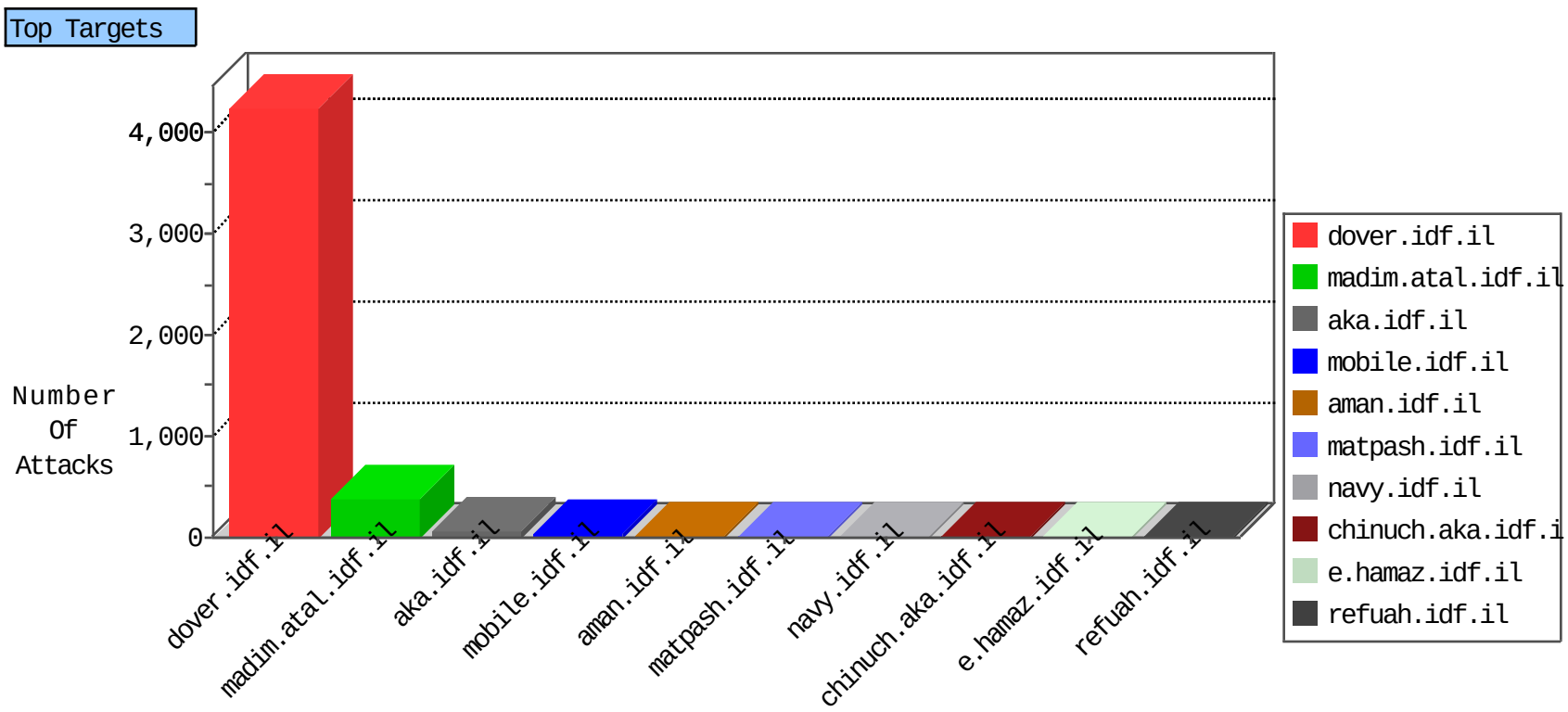
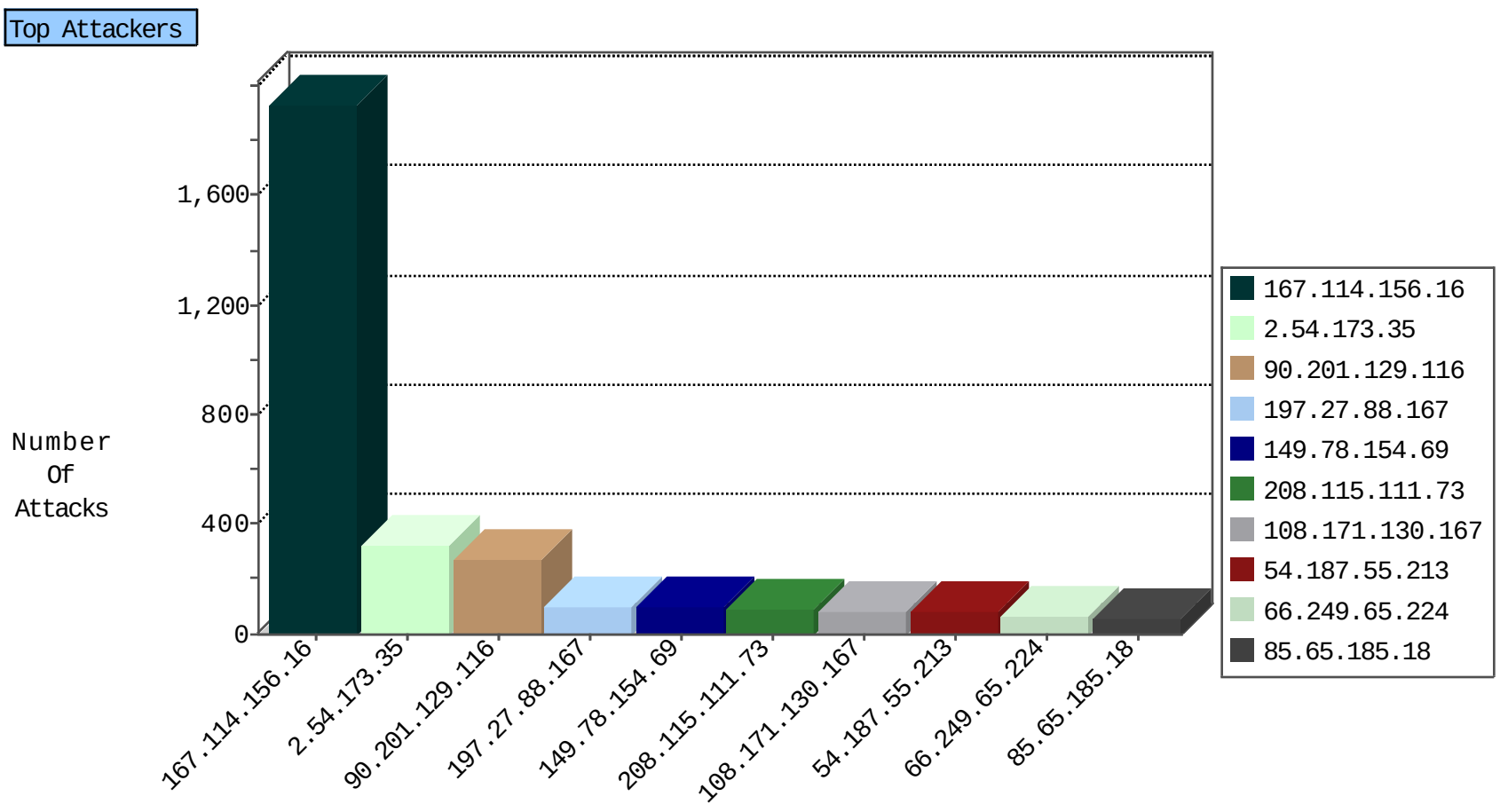
11-06-2015-22:04:07 to 11-06-2015-23:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-06-2015-22:04:07 to 11-06-2015-23:04:07

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	DOS-Tool-SwitchbladG	dest-reset	3152
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
212.116.172.230	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	28
82.166.22.98	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
109.66.113.28	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	21
109.66.113.28	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
2.54.23.114	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
93.173.230.238	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
80.246.136.204	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
79.177.207.253	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.13.15.74	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
176.13.6.15	Israel	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
79.176.192.90	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
85.250.51.47	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
46.19.86.253	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
46.19.86.253	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
187.188.166.208	Mexico	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
71.6.158.166	United States	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
187.188.166.208	Mexico	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
176.13.7.29	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
54.244.22.103	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
149.78.198.240	Israel	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1

11-06-2015-22:04:07 to 11-06-2015-23:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-06-2015-22:04:07 to 11-06-2015-23:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	**Signature**	**Count**

11-06-2015-22:04:07 to 11-06-2015-23:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
90.201.129.116	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	271
197.27.88.167	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	99
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	97
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	89
108.171.130.167	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	86
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	78
169.204.238.174	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
77.125.135.103	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
85.65.185.18	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
176.13.19.76	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
65.119.29.42	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	44
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
66.249.65.231	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
2.102.9.66	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
66.249.65.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
2.54.173.35	Israel	147.237.0.19	madim.atal.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
5.29.69.119	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
185.58.201.28	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
66.249.65.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
84.108.92.109	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
2.52.63.73	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
79.250.94.154	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
82.166.22.98	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
162.243.199.26	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
79.182.106.113	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
108.85.69.221	United States	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
46.19.86.63	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
121.54.54.155	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
162.243.73.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.13.17.115	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
85.250.178.137	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
69.175.127.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
100.100.54.216		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
79.181.5.146	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
5.34.167.77	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
157.55.39.63	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
109.66.113.28	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
188.165.15.14	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
66.249.65.231	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9

11-06-2015-22:04:07 to 11-06-2015-23:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.173.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	233
2.54.173.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	64
80.246.137.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
93.172.145.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
5.158.236.247	Russian Federation	147.237.72.166	aka.idf.il	PHP Attempt	Block	6
5.158.236.247	Russian Federation	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 5.158.236.247	Block	5
80.246.136.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
40.77.167.63	United States	147.237.76.147	chinuch.aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	3
80.246.139.197	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.120.155.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
40.77.167.91	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.238	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/900-he/chinuch.aspx	Block	1
62.210.88.201	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to 51.254.206.142/httptest.php	Block	1
157.55.39.63	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/	Block	1
79.178.27.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
66.249.67.147	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
66.249.64.113	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
66.249.78.18	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1486-he/atal.aspx	Block	1
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
66.220.146.22	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/images/temp/password_image.jpg	Block	1
157.55.39.78	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/qsystemform/	Block	1
79.182.226.246	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
2.54.128.12	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.67.202	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_pictures.asp	Block	1
46.121.40.158	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
85.65.12.164	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
68.180.228.112	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
66.249.64.51	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 66.249.64.51	Block	1
80.230.93.138	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
46.19.85.167	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
2.54.161.198	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.67.208	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/7/x©x§x•x¤x™xª 7	Block	1
59.52.158.27	China	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/miluim/about.aspx	Block	1
93.172.14.162	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	1
5.158.236.247	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/index.php	Block	1
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
207.46.13.1	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
66.249.64.56	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/2431.jpg	Block	1
46.19.85.167	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method x55 in URL	Block	1
66.249.67.238	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
59.52.158.27	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
77.127.222.23	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1

11-06-2015-22:04:07 to 11-06-2015-23:04:07