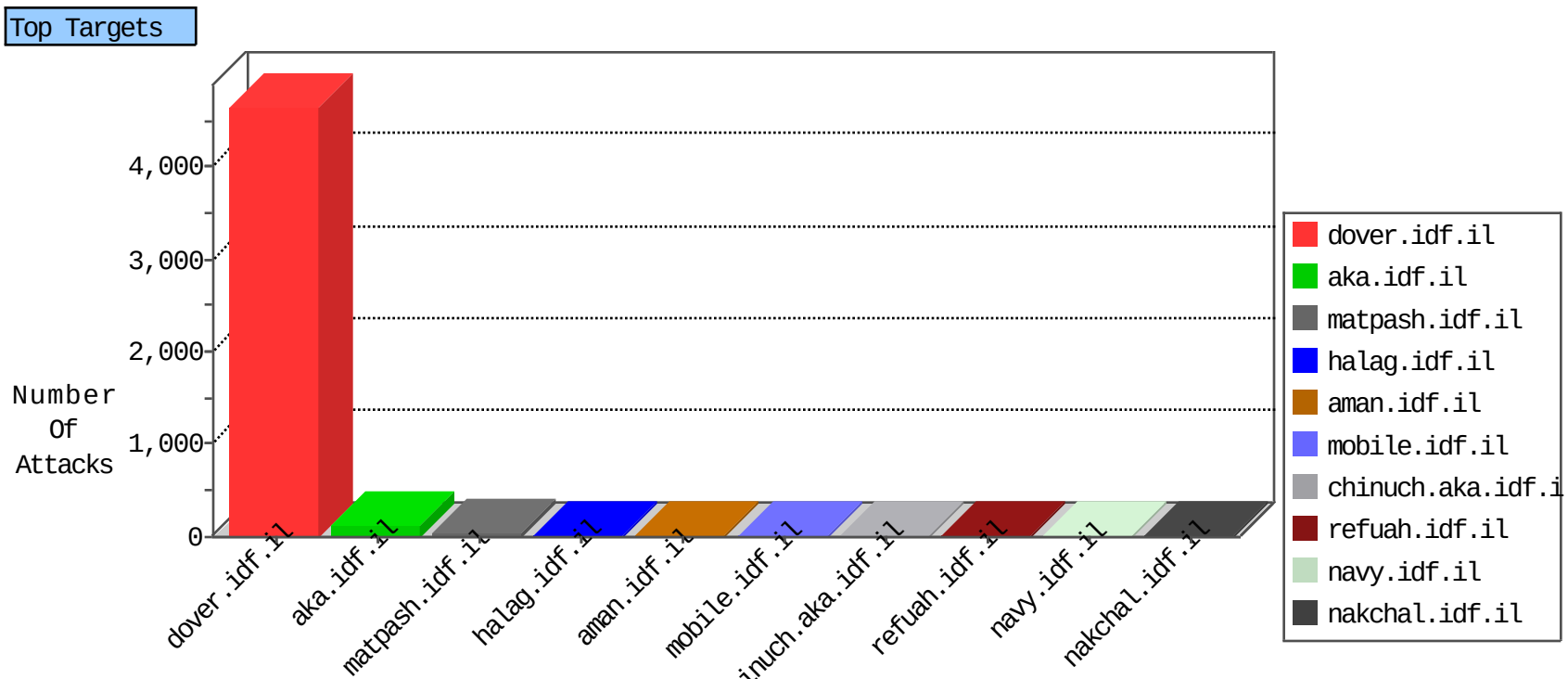
11-06-2015-08:04:01 to 11-06-2015-09:04:01

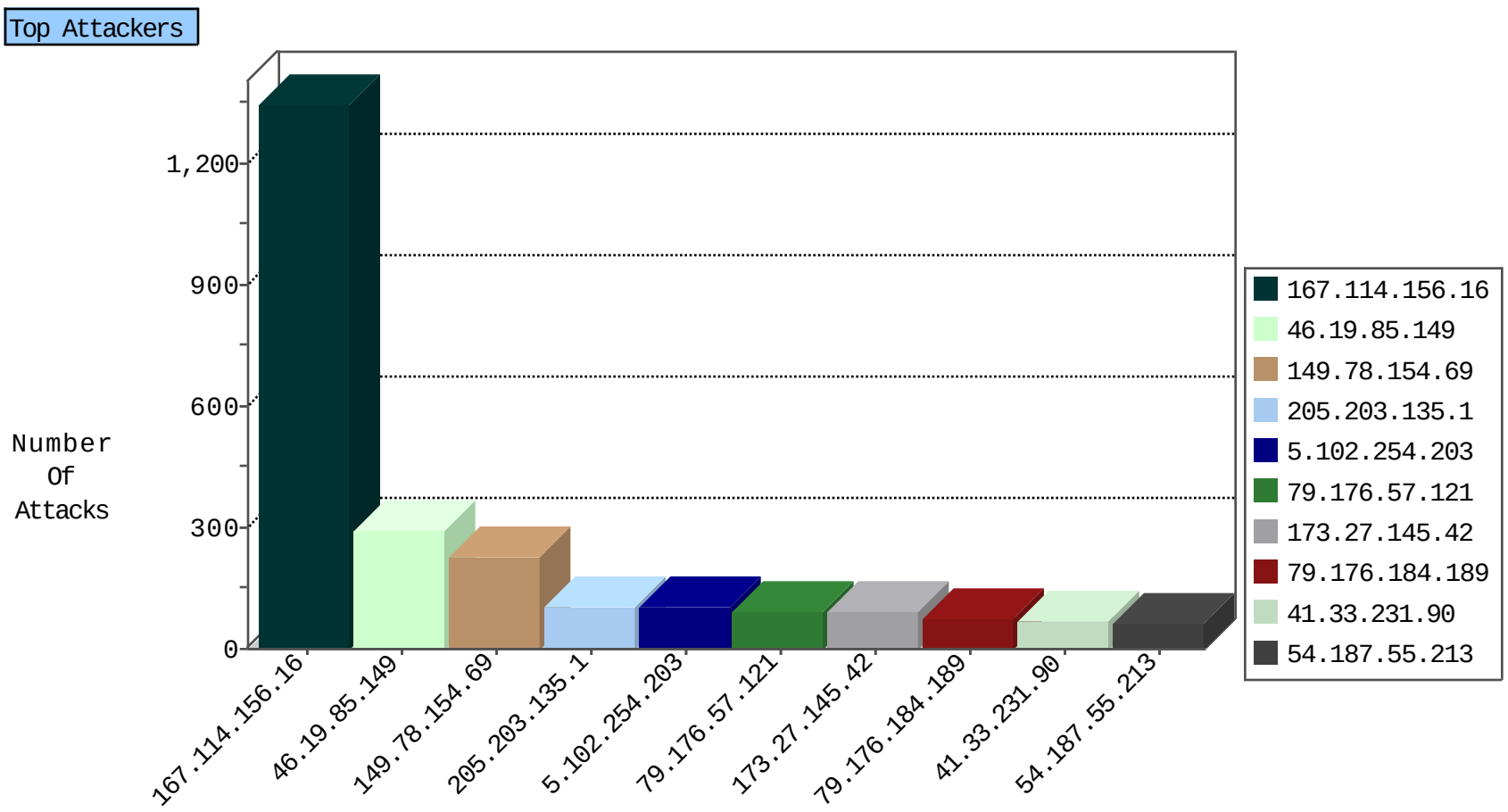
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

11-06-2015-08:04:01 to 11-06-2015-09:04:01

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	6150
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2486
66.249.67.67	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	422
37.142.64.49	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	41
46.19.86.134	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
2.52.57.126	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
46.19.86.134	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
79.176.159.189	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
79.182.103.91	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
188.120.150.249	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
109.160.191.92	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
79.177.166.131	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
124.11.242.216	Taiwan	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	3
109.65.170.72	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
84.111.124.91	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
37.142.242.131	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
157.55.12.64	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
93.172.185.98	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
2.54.162.7	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

11-06-2015-08:04:01 to 11-06-2015-09:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-06-2015-08:04:01 to 11-06-2015-09:04:01

Top Attackers In IDS

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

11-06-2015-08:04:01 to 11-06-2015-09:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.149	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	288
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	224
205.203.135.1	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	102
79.176.57.121	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	92
173.27.145.42	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	88
79.176.184.189	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	73
115.164.208.165	Malaysia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	60
54.187.55.213	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	60
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	55
68.96.59.120	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	55
77.126.236.228	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	54
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	49
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	47
84.108.34.55	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	45
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	45
185.58.201.28	Lebanon	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	44
2.54.54.226	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	43
82.145.211.76	Europe	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	43
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	41
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	39
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	34
86.67.9.88	France	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	34
212.199.182.150	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	33
46.19.85.132	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	32
93.172.160.154	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	25
195.34.150.18	Austria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	25
46.19.86.206	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
85.64.82.40	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
207.241.229.190	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	22
2.52.57.126	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
2.54.151.117	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
176.106.226.158	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
46.19.85.160	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	19
157.55.39.92	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	19
46.19.86.8	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	19
70.198.41.99	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
176.12.143.127	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
157.55.39.180	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
66.249.69.42	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
2.54.150.75	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
79.181.5.146	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
188.120.150.249	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
5.102.254.203	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
192.115.29.213	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
157.55.39.115	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
2.52.58.20	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
79.182.120.211	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
198.58.102.158	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
65.55.210.128	United States	147.237.77.234	halag.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14

11-06-2015-08:04:01 to 11-06-2015-09:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.102.254.203	Israel	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 5.102.254.203	Block	25
5.102.254.203	Israel	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 5.102.254.203	Block	25
5.102.254.203	Israel	147.237.77.216	dover.idf.il	Multiple Malformed URL from 5.102.254.203	Block	25
66.249.65.93	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	4
40.77.167.91	United States	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	3
149.78.191.61	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	3
176.12.147.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.67.36.233	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	2
72.9.148.10	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	2
79.176.159.189	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	2
5.29.252.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
157.55.39.31	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/site/links.aspx	Block	1
79.182.139.232	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
66.249.69.34	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
62.210.88.201	France	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.google.pl/search	Block	1
5.102.254.203	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
66.249.65.99	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.47	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim/templates/www.behazdaa.org	Block	1
82.102.169.113	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
5.102.254.203	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method Host: in URL www.idf.il	Block	1
66.249.69.42	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
192.99.16.165	Canada	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wordpress/wp-admin/	Block	1
66.249.67.133	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1644-he/refuah.aspx	Block	1
109.205.114.54	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
62.219.161.81	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
5.102.254.203	Israel	147.237.77.216	dover.idf.il	Malformed URL www.idf.il	Block	1
72.29.127.17	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/old/wp-admin/	Block	1
66.249.67.250	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
66.249.65.174	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
157.55.39.94	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
84.109.10.117	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
66.249.69.42	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush	Block	1
207.46.13.27	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/sip_storage/	Block	1
66.249.67.142	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/2689.jpg	Block	1
66.249.65.17	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71538-he/maarachot.aspx	Block	1
142.54.187.46	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.cloud.ph/	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	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
157.55.39.132	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/sip_storage/	Block	1
87.69.136.33	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
54.162.137.101	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
2.54.3.195	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.69.48	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/templates/sendtofriend/sendtofriend.aspx	Block	1
208.113.234.185	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp/wp-admin/	Block	1
66.249.67.196	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/163-4526-he/patzar.aspx	Block	1
66.249.65.86	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
79.181.52.117	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1

11-06-2015-08:04:01 to 11-06-2015-09:04:01