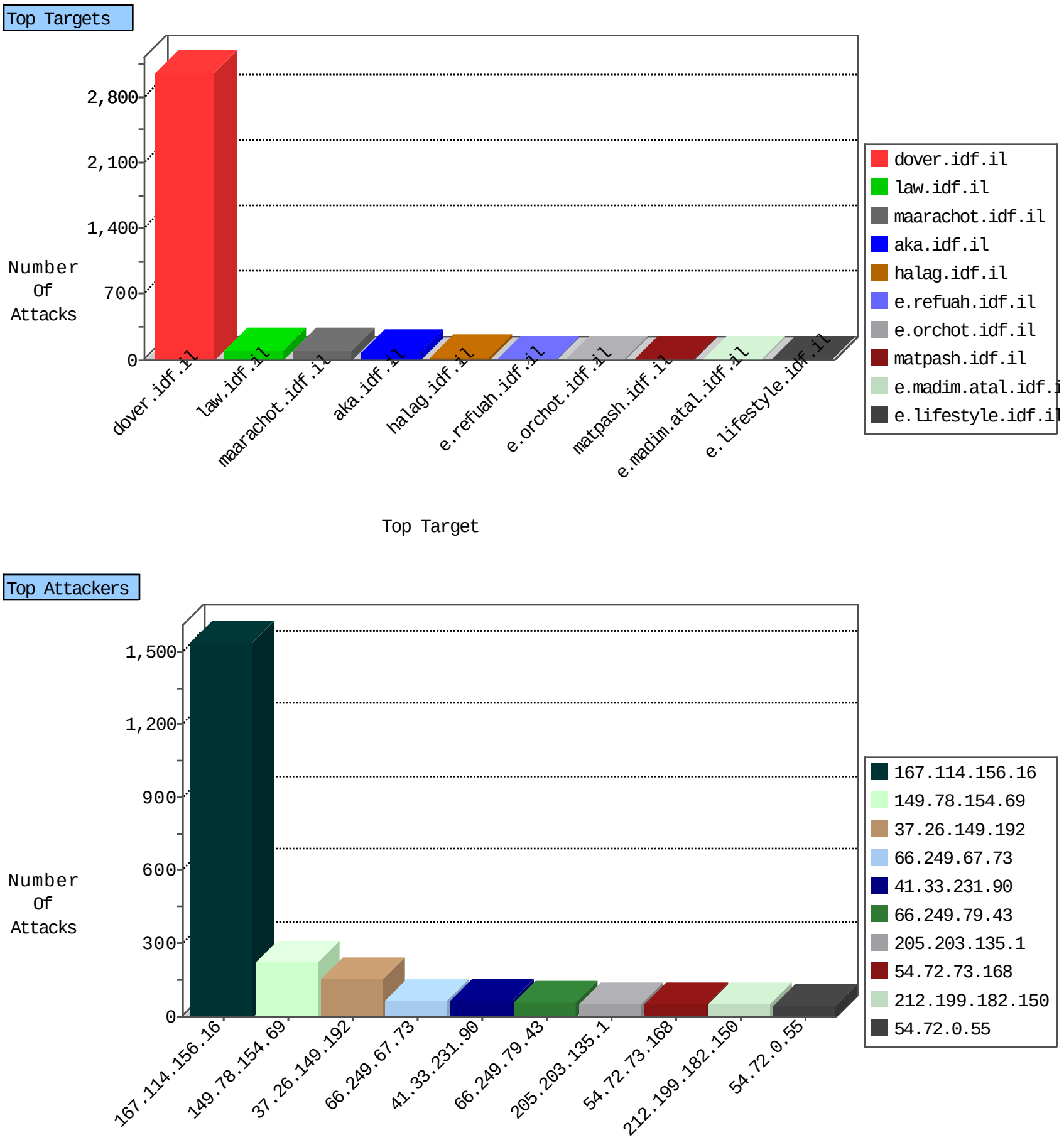
11-05-2015-03:04:03 to 11-05-2015-04:04:03

IDF Under Attack Daily Report



11-05-2015-03:04:03 to 11-05-2015-04:04:03

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	78725
66.249.67.73	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	15290
66.249.79.43	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	13504
66.249.79.41	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	5633
66.249.79.45	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	5180
207.46.13.93	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4631
66.249.79.13	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	4155
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3960
66.249.67.67	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3342
66.249.65.231	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3066
66.249.65.238	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2980
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2643
66.249.79.10	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2567
208.115.113.89	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2523
66.249.67.202	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2474
66.249.79.14	United States	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	2356
17.142.152.86	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2347
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2063
64.46.23.242	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1889
50.87.144.145	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1167
70.44.57.172	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1096
108.59.253.71	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	224
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	14
66.249.79.16	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	9
66.249.67.79	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	6
24.79.112.251	Canada	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
66.249.67.240	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	4
66.249.67.219	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	3
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
17.142.152.110	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
66.249.65.224	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
185.101.107.189		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
17.142.152.81	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
207.46.13.177	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
206.196.184.80	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
66.249.79.78	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1
71.6.186.90	United States	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
206.125.47.16	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
114.23.235.133	New Zealand	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
66.249.79.80	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
80.235.142.77	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
158.130.6.191	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
66.249.90.117	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
66.249.79.20	United States	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	1
168.235.198.223	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
84.2.152.84	Hungary	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
66.249.79.76	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1
207.46.13.14	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
17.142.152.72	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

11-05-2015-03:04:03 to 11-05-2015-04:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-05-2015-03:04:03 to 11-05-2015-04:04:03

Top Attackers In IDS

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

11-05-2015-03:04:03 to 11-05-2015-04:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	221
37.26.149.192	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	99
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	55
205.203.135.1	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	51
212.199.182.150	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	49
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	48
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	44
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	44
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	34
185.101.107.189		147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	27
212.179.90.106	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
80.235.142.77	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
17.142.152.110	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	23
17.142.152.81	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	23
64.46.23.242	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
207.46.13.177	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
37.26.149.192	Israel	147.237.77.216	dover.idf.i	Bad TCP sequence		monitor	21
66.249.65.238	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
72.9.148.10	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
71.63.49.87	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	19
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	19
199.30.25.104	United States	147.237.77.234	halag.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
37.26.149.192	Israel	147.237.77.216	dover.idf.i	Bad TCP sequence	Invalid ACK number	alert	18
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
37.26.149.192	Israel	147.237.77.216	dover.idf.i	Bad TCP sequence	Invalid ACK number	monitor	15
108.59.253.71	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
168.235.198.223	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
46.19.86.151	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
176.12.141.66	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
70.193.252.59	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
40.77.167.59	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
220.238.32.14	Australia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
111.151.98.77	China	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
17.142.152.72	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
66.249.65.231	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
24.157.105.172	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
66.249.65.238	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
2.52.10.58	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
109.64.168.149	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
208.115.111.73	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
207.46.13.93	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
207.46.13.14	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7
17.142.152.86	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7
207.46.13.180	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7
114.23.235.133	New Zealand	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7
195.34.150.18	Austria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7
207.46.13.74	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7
17.142.152.89	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7
66.249.65.224	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7

11-05-2015-03:04:03 to 11-05-2015-04:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.178.30.150	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	6
79.178.30.150	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/pages/fan_status.php	Block	6
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
199.16.156.126	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/1/size220x0/17471.jpg	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
96.237.199.16	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.79.225	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
66.249.65.80	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
66.249.79.16	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/booklets.aspx	Block	1
31.154.146.162	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.79.232	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
66.249.65.86	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
217.69.133.226	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method GET for aka.idf.il/kamlar/contact/default.asp	Block	1
74.82.47.2	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
66.249.79.105	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/tmuna/	Block	1
141.212.122.112	United States	147.237.77.170	maarachot.idf.il	Multiple Malformed URL from 141.212.122.112	Block	1
68.180.228.112	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/â€Ž	Block	1
66.249.65.93	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.79.107	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
185.32.179.242	Israel	147.237.76.39	mobile.meitav.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtContent in mobile.meitav.idf.il/1494-he/meitav.aspx	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.65.99	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.79.109	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	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/size220x0/17467.jpg	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8919-he/refuah.aspx	Block	1
66.249.79.10	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
23.81.90.154	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/home/default.aspx	Block	1
85.93.218.204	Luxembourg	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	1

11-05-2015-03:04:03 to 11-05-2015-04:04:03