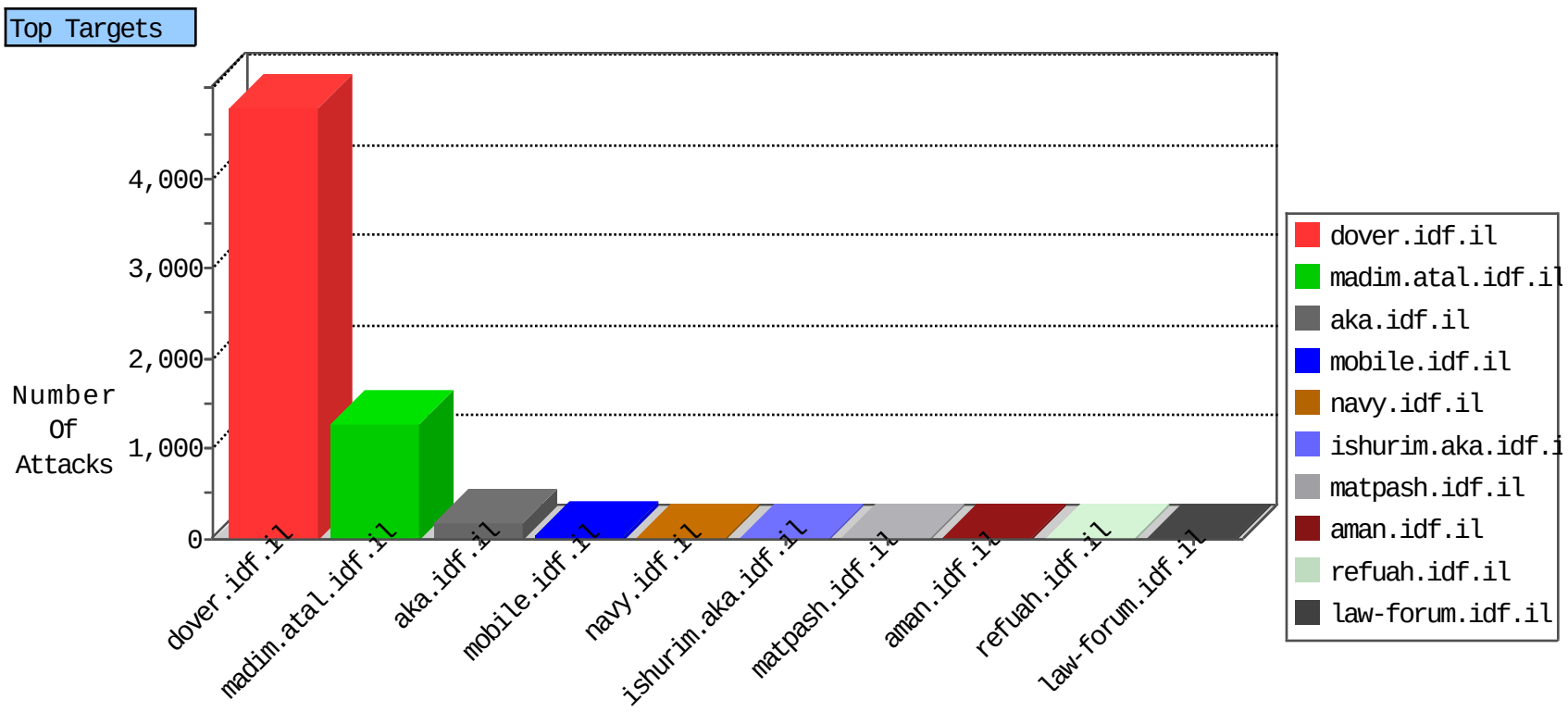
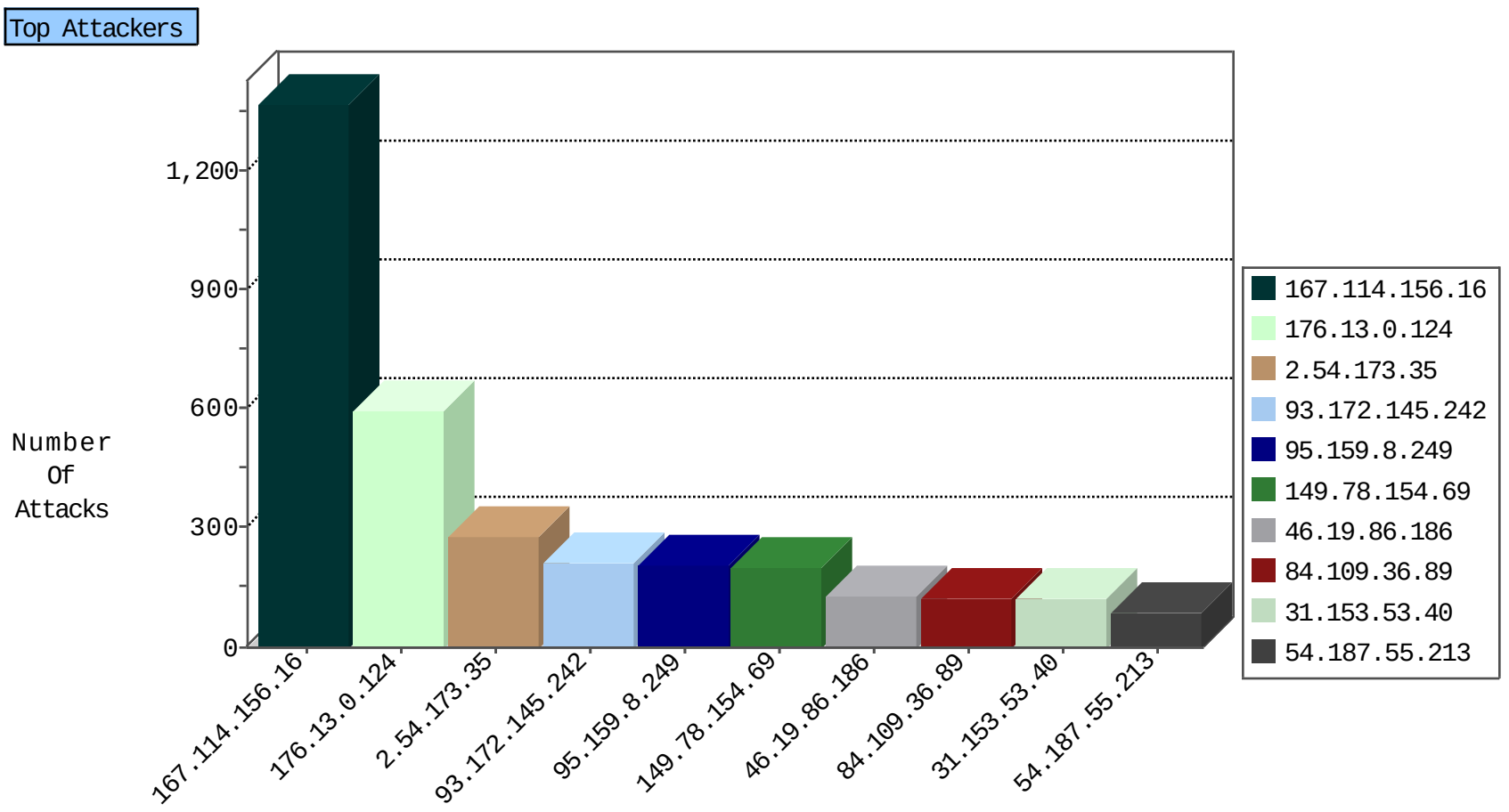
11-06-2015-21:04:02 to 11-06-2015-22:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-06-2015-21:04:02 to 11-06-2015-22:04:02

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	2629
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2360
220.181.108.97	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	233
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	33
46.120.3.29	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
93.173.182.168	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	18
87.68.62.185	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
12.232.97.226	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
5.22.131.106	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.52.35.195	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
82.205.94.187	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
77.125.103.18	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
80.246.136.162	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
185.120.126.36		147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
95.159.8.249	Syrian Arab Republic	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
89.138.95.138	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
109.186.35.36	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
47.17.178.232	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
2.54.173.35	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
2.54.173.35	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
79.177.132.112	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
46.166.188.68	Netherlands	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
78.52.228.106	Germany	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
79.181.143.35	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
46.166.188.68	Netherlands	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
78.52.228.106	Germany	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
91.208.115.34	Ukraine	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
79.177.50.45	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
146.185.239.100	Russian Federation	147.237.77.74	law.idf.il	block-sp-traf1	drop	1

11-06-2015-21:04:02 to 11-06-2015-22:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.178.221.92	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
79.183.128.84	Israel	147.237.72.166	aka.idf.il	C008: HTTP: Xenu UserAgent	Block	1

11-06-2015-21:04:02 to 11-06-2015-22:04:02

Top Attackers In IDS

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

11-06-2015-21:04:02 to 11-06-2015-22:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
95.159.8.249	Syrian Arab Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	204
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	202
84.109.36.89	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	122
31.153.53.40	Cyprus	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	122
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	69
85.65.166.32	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
79.179.128.126	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
54.244.22.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
79.181.153.41	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
46.121.42.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
87.68.74.180	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
91.23.167.210	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
109.67.14.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	40
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
197.32.221.189	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
142.169.78.198	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
201.116.16.177	Mexico	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
213.140.59.150	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
2.54.173.35	Israel	147.237.0.19	madim.atal.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
74.56.165.49	Canada	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	24
93.173.182.168	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
46.19.86.119	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
79.176.192.90	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
201.235.65.108	Argentina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
84.94.33.175	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
66.249.65.231	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
79.177.50.45	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
66.249.65.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
100.100.54.216		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
100.100.51.7		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
84.228.225.47	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
82.80.25.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
70.169.80.225	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
84.228.225.47	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
129.120.61.96	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
66.249.65.231	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14

11-06-2015-21:04:02 to 11-06-2015-22:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.0.124	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	317
176.13.0.124	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 176.13.0.124	Block	156
2.54.173.35	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	138
93.172.145.242	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	123
176.13.0.124	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	122
2.54.173.35	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	106
46.19.86.186	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	93
93.172.145.242	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	89
79.180.248.237	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	54
46.19.86.186	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	36
77.125.117.130	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	17
208.115.113.88	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on navy.idf.il/giyus/forum/asp/showforum.asp	Block	5
208.115.111.72	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	4
37.142.238.133	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.54.173.35	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	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
176.13.7.196	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.249.65.18	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
207.232.37.228	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
132.170.27.255	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-en/dover.aspx	Block	2
66.249.64.61	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/3141.jpg	Block	1
95.252.33.104	Italy	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
84.108.36.112	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 84.108.36.112	Block	1
66.249.67.250	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
192.115.100.190	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/edim/library/generaldoc.asp	Block	1
157.55.39.63	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
91.79.181.51	Russian Federation	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
62.210.88.201	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 51.254.206.142/httptest.php	Block	1
79.176.203.48	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	1
176.13.0.124	Israel	147.237.0.19	madim.atal.idf.i	Too Many 403: Response Code per Session	Block	1
66.249.67.132	Israel	147.237.72.166	aka.idf.il	Unauthorized Method GET for aka.idf.il/iturim/asp/searchresults.asp	Block	1
66.249.64.108	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/0/770.pdf	Block	1
105.154.181.142	Morocco	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
84.108.36.112	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/sip_storage/	Block	1
37.237.140.67	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	1
207.46.13.172	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.242	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/robots.txt	Block	1
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.238	Block	1
91.79.181.51	Russian Federation	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
66.249.64.26	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/2908.pdf	Block	1
208.115.111.73	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/14-he	Block	1
79.180.114.19	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush	Block	1
66.249.67.147	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	1
66.249.64.113	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/7/267.pdf	Block	1
109.65.72.100	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
84.228.225.47	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
46.19.85.131	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/kamlar	Block	1
77.88.31.157	Russian Federation	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
207.46.13.172	United States	147.237.72.166	aka.idf.il	Unknown Parameter tm in www.aka.idf.il/main/giyus/	None	1

11-06-2015-21:04:02 to 11-06-2015-22:04:02