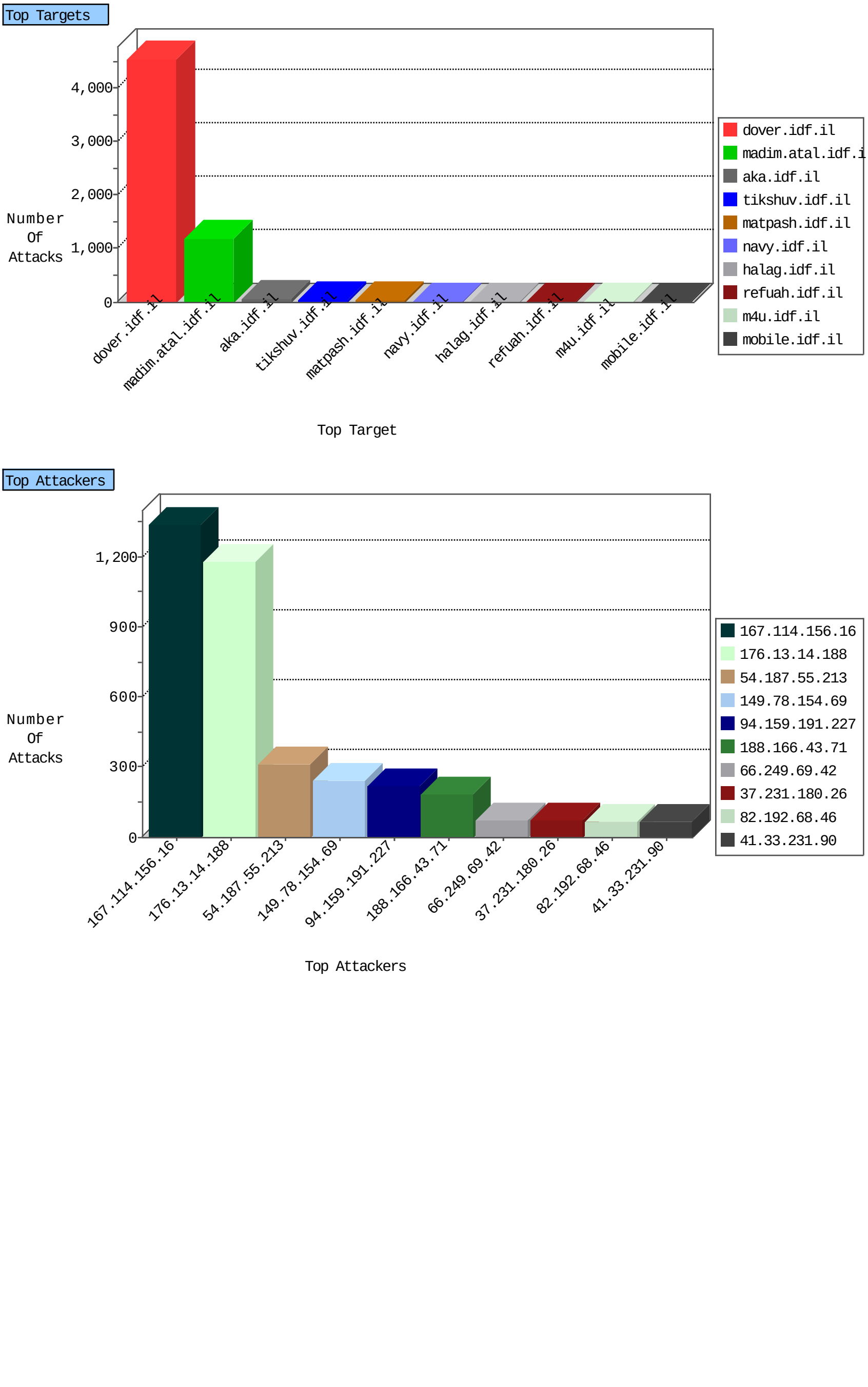
11-06-2015-07:04:01 to 11-06-2015-08:04:01

IDF Under Attack Daily Report



11-06-2015-07:04:01 to 11-06-2015-08:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.79	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3861
149.78.154.69	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3180
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2320
66.249.67.13	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1890
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	491
66.249.67.6	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	382
213.57.202.92	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
194.90.83.233	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
204.42.253.2	United States	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	3
78.108.161.226	Lebanon	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
108.211.9.98	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
180.97.106.161	China	147.237.72.166	aka.idf.il	block-sp-traf1	drop	1
46.19.86.85	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

11-06-2015-07:04:01 to 11-06-2015-08:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
63.143.34.37	United States	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	1
63.143.34.37	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

11-06-2015-07:04:01 to 11-06-2015-08:04:01

Top Attackers In IDS

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

11-06-2015-07:04:01 to 11-06-2015-08:04:01

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	240
94.159.191.227	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	217
188.166.43.71	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	186
37.231.180.26	Kuwait	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	72
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	69
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	65
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
46.116.88.101	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
185.58.201.28	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
2.52.61.27	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
176.13.14.188	Israel	147.237.0.19	madim.atal.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	49
91.232.101.58	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
109.67.129.236	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
176.13.7.240	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
66.249.69.42	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	40
68.96.59.120	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
31.154.29.94	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
98.202.189.179	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
157.55.39.180	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
64.46.23.242	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
109.65.114.222	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
2.54.12.68	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
46.120.251.104	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
66.249.69.42	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
5.62.128.68	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
157.55.39.181	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
46.19.86.215	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
66.249.69.34	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
212.70.38.146	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
157.55.39.208	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
157.55.39.115	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
66.249.69.26	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
82.80.25.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
157.55.39.92	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
66.249.69.26	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
79.179.59.247	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
66.249.69.34	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
66.249.69.34	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
198.58.102.156	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
213.57.130.227	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
46.19.85.24	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
84.109.243.29	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12

11-06-2015-07:04:01 to 11-06-2015-08:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.14.188	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.14.188	Block	782
176.13.14.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	335
173.208.169.34	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 173.208.169.34	Block	25
176.13.14.188	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 176.13.14.188	Block	14
173.208.169.34	United States	147.237.0.34	tikshuv.idf.il	Multiple Admin Blocking from 173.208.169.34	Block	13
173.208.169.34	United States	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	8
162.243.215.132	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 162.243.215.132	Block	3
2.52.151.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	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
198.20.69.74	United States	147.237.0.19	madim.atal.idf.il	Distributed Unauthorized URL Access on 147.237.0.19/	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/9/3049.jpg	Block	1
40.77.167.14	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/sip_storage/	Block	1
85.250.3.125	Israel	147.237.0.19	madim.atal.idf.il	Cookie Tampering on cookie _pk_ref.322.9cd2: Expected ["","",1445274878,"https://www.google.co.il/"], Observed ["","",1446788915,"https://www.google.co.il/"]	None	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
66.102.9.81	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
157.55.39.189	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/navmenu/	Block	1
72.9.148.10	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 72.9.148.10	Block	1
66.249.67.190	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
207.46.13.71	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-11019-en/cogat.aspx.	Block	1
40.77.167.21	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	1
92.53.113.220	Russian Federation	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/test/wp-admin/	Block	1
66.249.67.254	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/3/2413.jpg	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
72.9.148.10	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/120103-3.stm)	Block	1
66.249.67.224	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
207.46.13.120	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
40.77.167.39	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
173.208.169.34	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/freeaspupload/uploadtester.asp	Block	1
93.173.233.105	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
190.232.70.148	Peru	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/default.aspx	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
2.52.184.84	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
173.208.169.34	United States	147.237.0.34	tikshuv.idf.il	Admin Blocking	Block	1
79.176.165.53	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
66.249.67.240	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
212.227.114.135	Germany	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-admin/	Block	1
62.210.88.201	France	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to www.google.pl/search	Block	1
151.80.31.125	Italy	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
66.249.69.34	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
198.20.69.74	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
66.249.67.133	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/3250.jpg	Block	1
5.28.178.213	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
82.82.42.178	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
176.13.14.188	Israel	147.237.0.19	madim.atal.idf.il	Too Many 403: Response Code per Session	Block	1
62.210.88.201	France	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 51.254.206.142/httptest.php	Block	1
157.55.39.104	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/sip_storage/	Block	1

11-06-2015-07:04:01 to 11-06-2015-08:04:01