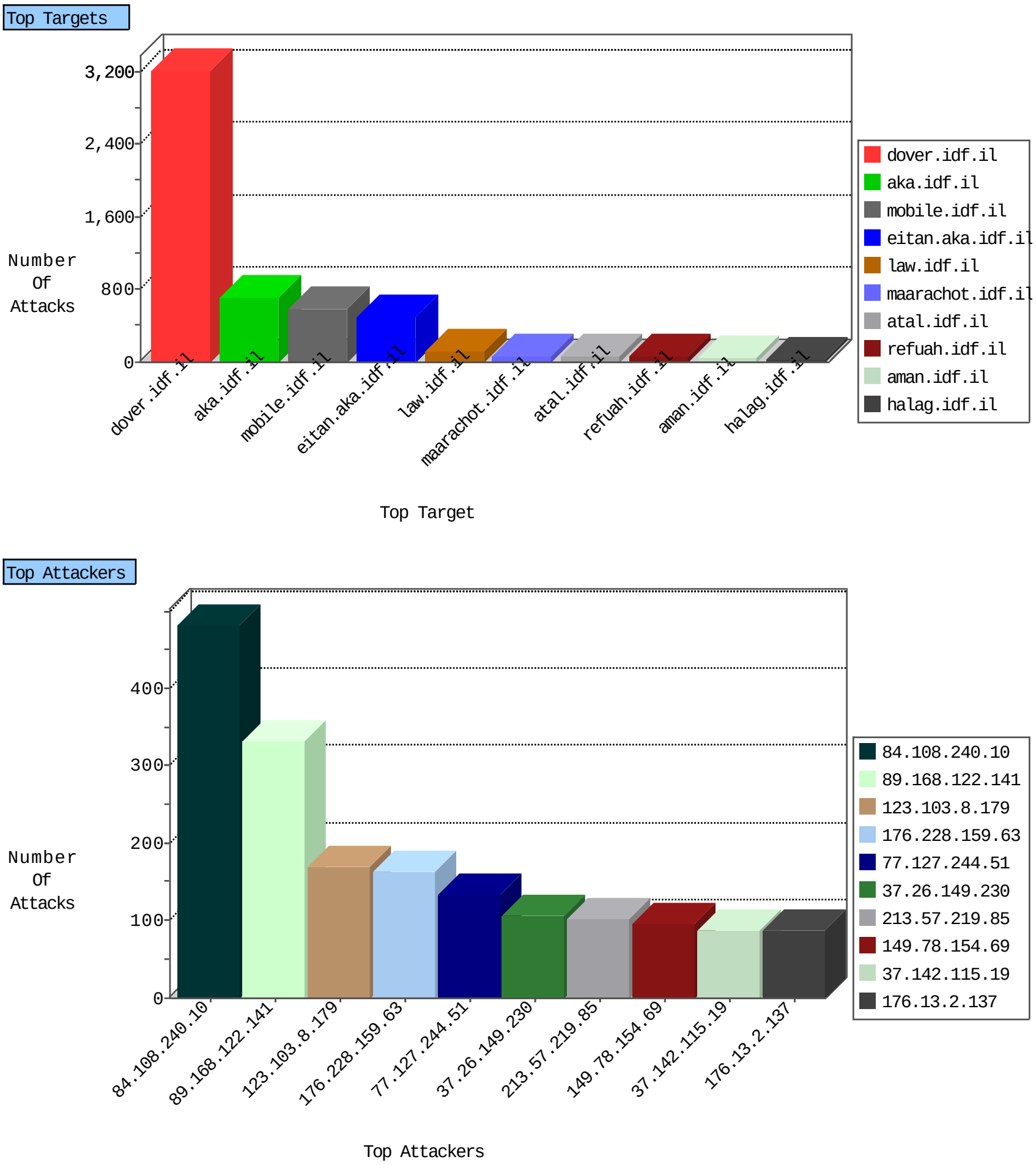
10-31-2015-14:04:04 to 10-31-2015-15:04:04

IDF Under Attack
Daily Report



10-31-2015-14:04:04 to 10-31-2015-15:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1438
66.249.67.34	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	826
66.249.67.32	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	479
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	125
66.249.69.84	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	68
66.249.69.76	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	61
37.142.68.131	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	46
37.142.115.19	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	39
81.218.234.122	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
31.154.91.45	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
82.166.22.58	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	23
176.13.7.20	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
41.33.231.82	Egypt	147.237.77.216	dover.idf.il	SYN Flood full table	drop	19
149.78.191.141	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
109.66.200.254	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
46.121.118.103	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
79.182.32.246	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
87.112.137.72	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
79.179.177.207	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
46.19.86.193	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
188.161.50.224	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
176.12.148.201	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
109.67.124.160	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
84.108.56.167	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
79.176.179.34	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
149.88.183.205	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
79.180.201.35	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
85.64.4.181	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
81.218.234.122	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
123.103.8.179	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
93.172.63.22	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
84.109.1.219	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
176.228.159.63	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
94.230.86.180	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
93.172.157.116	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
84.111.70.62	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
80.76.173.191	Qatar	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
89.168.122.141	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
46.19.85.187	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.120.51.211	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
37.26.149.164	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
79.182.130.134	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.54.40.133	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.13.0.196	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
149.78.147.160	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
185.32.179.143	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
84.228.70.225	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.106.46.74	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
2.52.153.223	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
70.126.106.13	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3

10-31-2015-14:04:04 to 10-31-2015-15:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
94.102.153.58	United Kingdom	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	20
74.208.66.220	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	3
23.99.3.151	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	1

10-31-2015-14:04:04 to 10-31-2015-15:04:04

Top Attackers In IDS

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

10-31-2015-14:04:04 to 10-31-2015-15:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
89.168.122.141	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	328
123.103.8.179	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	162
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	96
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	64
149.78.147.160	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
46.19.85.203	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
176.13.9.226	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
80.187.106.50	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
2.52.143.29	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	50
109.64.208.153	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
109.66.181.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
79.178.135.125	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	40
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
37.142.115.19	Israel	147.237.76.42	refuah.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
185.120.126.53		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
85.64.15.195	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
37.26.149.230	Israel	147.237.77.243	mobile.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
100.100.83.106		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	27
176.214.79.155	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
84.154.18.59	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
46.19.86.54	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
37.142.115.19	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
176.228.159.63	Israel	147.237.77.243	mobile.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
87.106.184.160	Germany	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	20
223.227.248.215	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
80.246.130.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
151.80.31.112	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
74.208.66.220	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	19
100.100.78.50		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
79.182.212.243	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	17
80.246.130.136	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
81.218.235.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
66.249.93.196	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
85.250.64.244	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
46.121.118.103	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
85.64.56.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
41.102.239.58	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
66.249.78.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
100.100.17.109		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
93.95.201.218	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.228.159.63	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	135
77.127.244.51	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.127.244.51	Block	120
213.57.219.85	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	90
176.13.2.137	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	75
37.26.149.230	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	74
179.43.138.75	Switzerland	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/homepage/	Block	60
85.64.4.181	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	57
31.168.200.178	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	45
79.177.198.8	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	30
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	30
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19748-he/idfgdover.aspx	Block	15
66.249.67.132	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sites/resources/chinuch	Block	15
93.172.63.22	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 93.172.63.22	Block	15
46.120.120.176	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	15
203.217.130.65	Malaysia	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
66.249.69.89	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1407-he/atal.aspx	Block	15
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	15
109.67.145.191	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/talpiotquestionnaire.aspx	None	15
37.142.115.19	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	15
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/style/shared/reset.css	Block	15
66.249.67.143	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/2/107072.pdf	Block	15
93.172.63.22	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	15
66.249.65.28	Israel	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/shared/usercontrols/navmenu/	Block	15
77.127.244.51	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	15
213.57.36.250	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	15
66.249.69.97	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1493-he/atal.aspx	Block	15
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	15
151.43.41.227	Italy	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
85.65.143.13	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	15
46.116.110.245	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$emailUpdate$hiddenUpdateEmail in www.aka.idf.il/main/giyus/faq.aspx	None	15
66.249.78.247	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/	Block	15
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	15
93.172.142.250	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	15
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/×©×§×•×¤×™×ª 13	Block	15
31.184.238.55	Russian Federation	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/6/106906.pdf	Block	15
79.177.190.209	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	15
66.249.78.4	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	15
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	15
151.80.31.112	Italy	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
87.69.225.127	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	15
46.116.222.152	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	15
68.180.228.59	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/general/youtu.be/dsh2chqxxt0	Block	15
189.38.90.212	Brazil	147.237.72.166	aka.idf.il	MSSQL Data Retrieval with Implicit Conversion Errors	None	15
66.249.67.247	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71822-he/maarachot.aspx	Block	15
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx	Block	15
105.102.31.23	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/login	Block	15
31.210.176.40	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	15
66.249.78.59	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	15
66.249.67.77	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/scriptresource.axd	Block	15
157.55.39.83	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/iturim/asp/displayonesoldier.asp	None	15