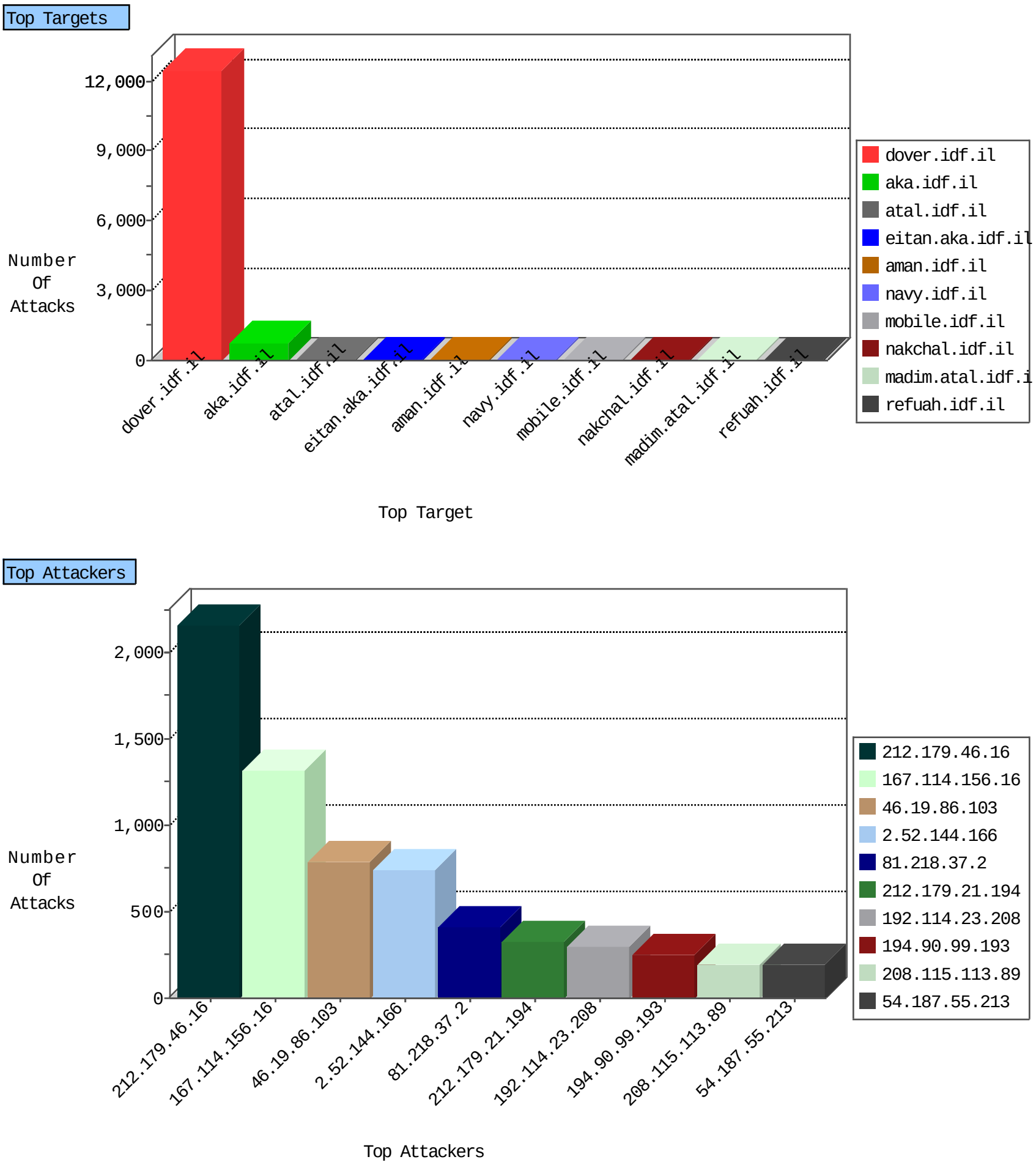
11-05-2015-13:04:06 to 11-05-2015-14:04:06

IDF Under Attack Daily Report



11-05-2015-13:04:06 to 11-05-2015-14:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.37.2	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	2561
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1996
66.249.67.67	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	475
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	238
66.249.67.194	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	237
2.54.161.10	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	85
2.52.144.166	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	85
212.25.83.133	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	48
176.13.7.243	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	43
84.109.119.7	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
2.52.17.77	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	22
80.246.140.186	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	22
46.43.74.17	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	21
46.19.85.15	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
82.80.86.86	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
79.177.123.217	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
77.127.77.243	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
2.54.157.175	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10
46.19.86.129	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
176.228.140.137	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
41.164.25.50	South Africa	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
176.13.5.226	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
83.149.99.157	Netherlands	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	6
213.207.85.100	Netherlands	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
66.249.79.43	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	6
176.13.0.72	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
46.116.171.174	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
213.151.61.247	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
81.218.140.102	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.19.86.245	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
109.66.164.7	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
80.246.139.252	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.54.151.160	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
79.177.113.92	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
176.12.139.69	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
87.68.61.58	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
79.182.39.45	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.54.136.183	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.117.236.245	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
83.149.99.157	Netherlands	147.237.77.121	e.navy.idf.il	Invalid TCP Flags	drop	4
176.12.144.179	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
188.161.65.77	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
84.94.197.246	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.85.250	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
213.151.48.138	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
209.88.198.1	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
81.218.199.247	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3

11-05-2015-13:04:06 to 11-05-2015-14:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

11-05-2015-13:04:06 to 11-05-2015-14:04:06

Top Attackers In IDS

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

11-05-2015-13:04:06 to 11-05-2015-14:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.46.16	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2159
46.19.86.103	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	786
2.52.144.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	671
192.114.23.208	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	295
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	250
194.90.99.193	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	248
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	192
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	186
91.181.136.87	Belgium	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	161
81.218.37.2	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	145
41.33.148.100	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	130
46.121.94.141	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	110
176.45.240.183	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	96
95.86.111.8	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	93
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	86
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	80
37.26.148.251	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	69
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
62.0.41.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
2.54.176.34	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
66.249.65.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
197.133.127.84	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
85.65.93.193	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
81.218.199.247	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
79.177.123.217	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
79.181.141.244	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
37.26.146.162	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
66.249.93.192	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
209.88.198.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
66.249.65.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
122.148.243.248	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
82.102.197.59	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
64.233.172.163	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
66.249.65.231	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
64.233.172.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
66.249.93.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
66.249.65.238	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
46.19.85.209	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
121.54.58.129	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
80.246.130.188	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
46.19.86.204	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	34
185.37.12.200	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
2.52.144.166	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	32

11-05-2015-13:04:06 to 11-05-2015-14:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.116.232.69	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	38
194.90.140.29	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 194.90.140.29	Block	18
2.54.136.183	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
185.120.126.27		147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	5
185.120.126.27		147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/pages/fan_status.php	Block	5
80.178.205.237	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 80.178.205.237	Block	4
46.19.85.80	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
5.102.254.224	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
62.0.100.86	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/default.asp	Block	2
87.68.33.217	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/pages/fan_status.php	Block	2
2.54.150.83	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.12.174	Israel	147.237.77.243	mobile.idf.il	Suspicious Response Code	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
2.52.24.35	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.86.61	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
87.68.33.217	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
66.249.79.107	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
176.13.18.73	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
142.54.174.67	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to www.cloud.ph/	Block	1
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	1
192.116.232.69	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter wb48617274 in www.eitan.aka.idf.il/style/shared/reset.css	None	1
66.249.79.236	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/default.asp	Block	1
176.13.12.174	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.65.251	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 66.249.65.251	Block	1
37.26.149.199	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
212.117.143.250	Israel	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	1
192.116.232.69	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter wb48617274 in www.eitan.aka.idf.il/shared/clientscripts/op/jqueryfunctions.js	None	1
66.249.79.109	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/4/71614.pdf	Block	1
185.120.126.1		147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.65.132	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/links.aspx	Block	1
149.78.212.198	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
82.80.17.163	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
192.116.232.69	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter wb48617274 in www.eitan.aka.idf.il/style/shared/text.css	None	1
192.116.232.69	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter wb48617274 in www.eitan.aka.idf.il/scriptresource.axd	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.65.251	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/general.aspx	Block	1
212.117.143.250	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/ajax/updatestatus.php	Block	1
87.69.81.241	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	1
192.116.232.69	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter wb48617274 in www.eitan.aka.idf.il/shared/clientscripts/ui/i18n/jquery-ui-i18n.js	None	1
80.178.205.237	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/sip_storage/files/3/size338x0/1613.jpg	Block	1
66.249.79.218	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
174.129.228.67	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
66.249.65.223	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
82.80.97.80	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
2.54.160.115	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.116.232.69	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter wb48617274 in www.eitan.aka.idf.il/shared/ajax/createcaptchaimage.aspx	None	1
176.13.15.81	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.chimush.atal.idf.il/994-8668-he/himudh.aspx	Block	1
66.249.67.67	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
46.19.85.126	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
217.31.48.30	Czech Republic	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/rom-0	Block	1

11-05-2015-13:04:06 to 11-05-2015-14:04:06