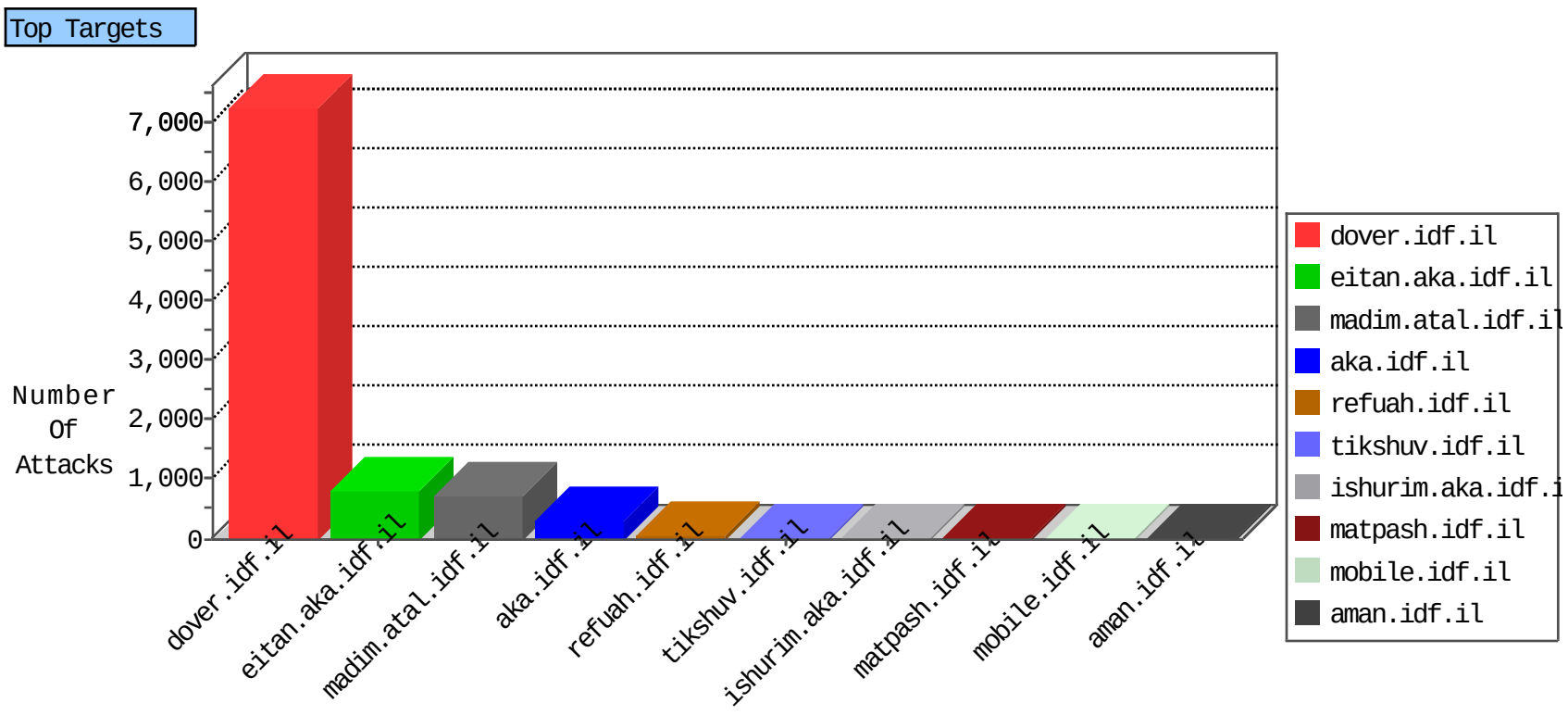
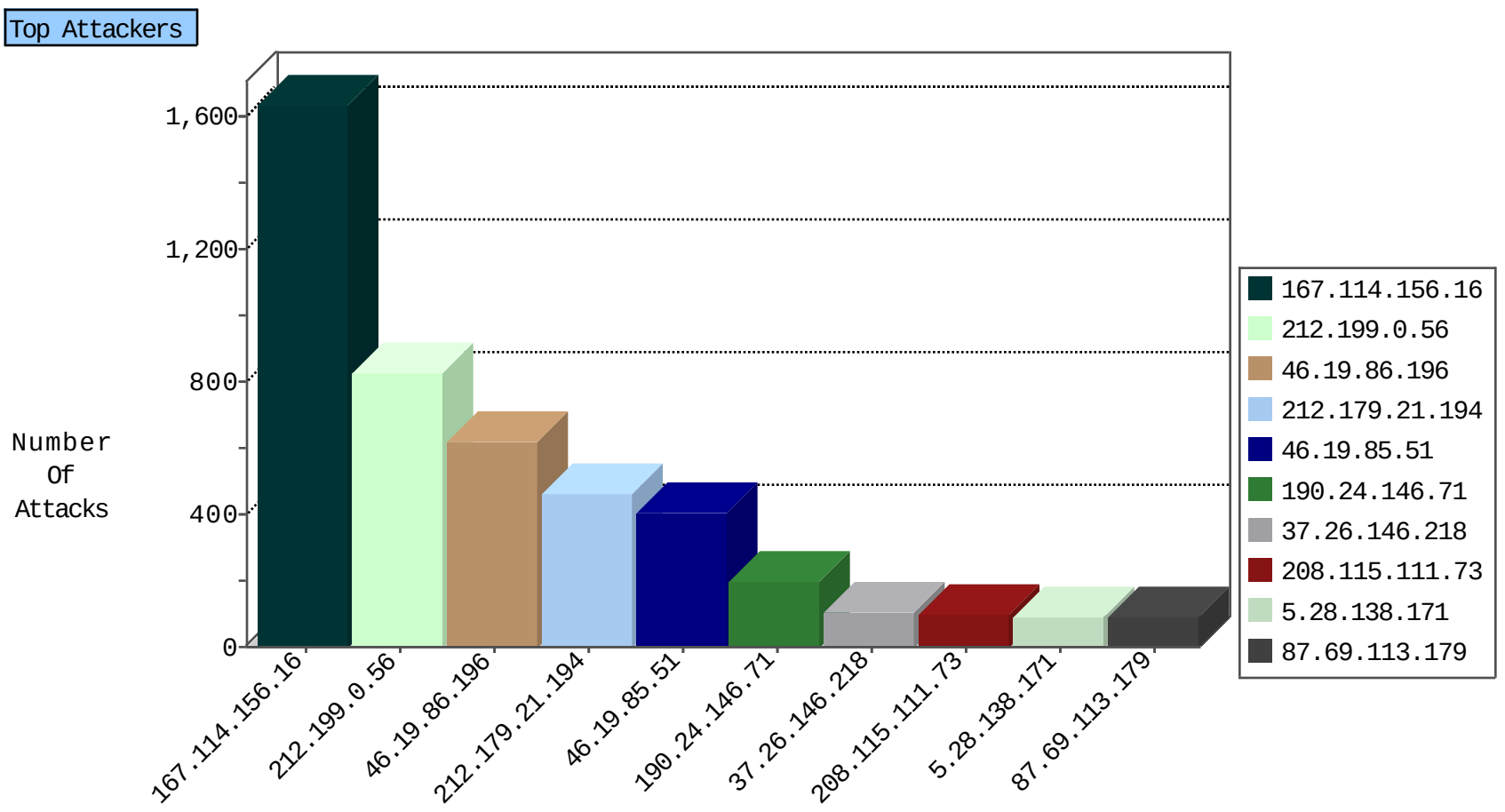
11-05-2015-16:04:07 to 11-05-2015-17:04:07

IDF Under Attack
Daily Report

Top Targets



Top Attackers



11-05-2015-16:04:07 to 11-05-2015-17:04:07

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	DOS-Tool-SwitchbladG	dest-reset	1891
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	908
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	442
46.19.85.51	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	304
194.90.128.25	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	84
69.248.86.176	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	49
85.64.0.181	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	41
2.54.148.235	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	37
80.178.231.215	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	35
80.230.29.141	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
46.117.133.72	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
176.13.1.218	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	29
37.26.149.145	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	28
81.218.234.122	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
109.160.133.128	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
80.178.148.59	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	24
82.145.218.62	Europe	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	20
46.19.86.139	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
79.182.133.87	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	18
176.13.1.218	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
176.13.14.204	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	18
95.86.99.91	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	18
2.54.35.253	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
37.142.128.154	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
212.179.46.16	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	13
91.228.127.198	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
132.73.203.152	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
149.78.252.180	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
79.235.16.150	Germany	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
81.218.235.10	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
149.78.146.84	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
109.66.179.98	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
176.13.4.101	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
79.181.96.217	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
37.26.149.151	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
82.145.218.155	Europe	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
109.67.198.122	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
37.26.147.160	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
77.127.255.197	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
31.168.197.129	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
85.65.19.112	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
149.78.246.236	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
176.13.19.208	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
84.190.159.232	Germany	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
2.54.25.135	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
37.26.148.129	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
46.116.221.66	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
81.218.235.10	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.19.85.129	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
176.13.15.183	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5

11-05-2015-16:04:07 to 11-05-2015-17:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.219.13.180	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	8262: HTTP: Slowloris DoS Tool	Block	1

11-05-2015-16:04:07 to 11-05-2015-17:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1

11-05-2015-16:04:07 to 11-05-2015-17:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.199.0.56	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	702
46.19.86.196	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	617
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	427
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	371
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	194
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	90
87.69.113.179	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	89
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
37.26.146.195	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	83
109.65.120.125	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	79
79.180.125.16	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	78
46.19.85.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
2.52.24.42	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
81.218.29.219	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
216.11.6.41	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
8.37.227.248	Anonymous Proxy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
168.235.194.52	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
72.69.44.227	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
176.13.1.218	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
46.19.85.205	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	35
82.145.218.62	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
176.13.11.225	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
188.120.134.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
77.127.255.197	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
66.249.69.26	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
67.198.136.219	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
79.235.16.150	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
95.86.99.91	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
66.249.82.88	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
194.90.128.25	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
66.249.82.94	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
79.181.96.217	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
2.52.175.214	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
62.183.125.49	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
176.13.14.204	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
105.202.124.69	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
5.28.138.171	Israel	147.237.0.19	madim.atal.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
79.180.58.177	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
2.36.95.249	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
74.56.165.49	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19

11-05-2015-16:04:07 to 11-05-2015-17:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	215
46.19.85.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	155
212.199.0.56	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 212.199.0.56	Block	123
37.26.146.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	90
5.28.138.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	61
176.13.20.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
176.13.5.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
37.26.146.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	17
176.13.18.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
5.28.138.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	12
46.19.86.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
89.138.251.4	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	5
79.180.52.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
89.138.251.4	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/pages/fan_status.php	Block	5
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	5
2.54.183.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.186.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.146.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.103	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
149.210.158.71	Netherlands	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 149.210.158.71	Block	3
46.19.85.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	3
176.13.18.150	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.18.150	Block	3
31.154.8.98	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.182.152.241	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.147.190	Israel	147.237.0.34	tikshuv.idf.il	Redundant HTTP Headers Referer	Block	1
192.99.13.116	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22909-ar/dover.aspx)	Block	1
176.12.141.129	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in atal.idf.il/1437-he/atal.aspx	Block	1
77.125.119.198	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.125.119.198	Block	1
122.224.8.111	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ckfinder	Block	1
66.249.69.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
66.249.65.17	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	1
212.76.121.245	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/https:/aka.idf.il/	Block	1
85.250.209.14	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	1
79.178.164.99	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/kesher/	Block	1
66.249.79.91	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/pratim/pirteyerua/	Block	1
167.114.172.229	Canada	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 167.114.172.229	Block	1
109.64.64.68	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
80.246.130.162	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
203.133.171.43	Korea, Republic of	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
77.125.119.198	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
66.249.69.42	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
141.212.122.64	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to /x	Block	1
66.249.65.80	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
212.199.0.56	Israel	147.237.76.200	eitan.aka.idf.il	Too Many 404: Response Code per Session	Block	1
87.69.113.179	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
79.178.199.126	Israel	147.237.72.166	aka.idf.il	Unknown Parameter _ in www.aka.idf.il/main/giyus/general.aspx	None	1
66.249.79.105	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1

11-05-2015-16:04:07 to 11-05-2015-17:04:07