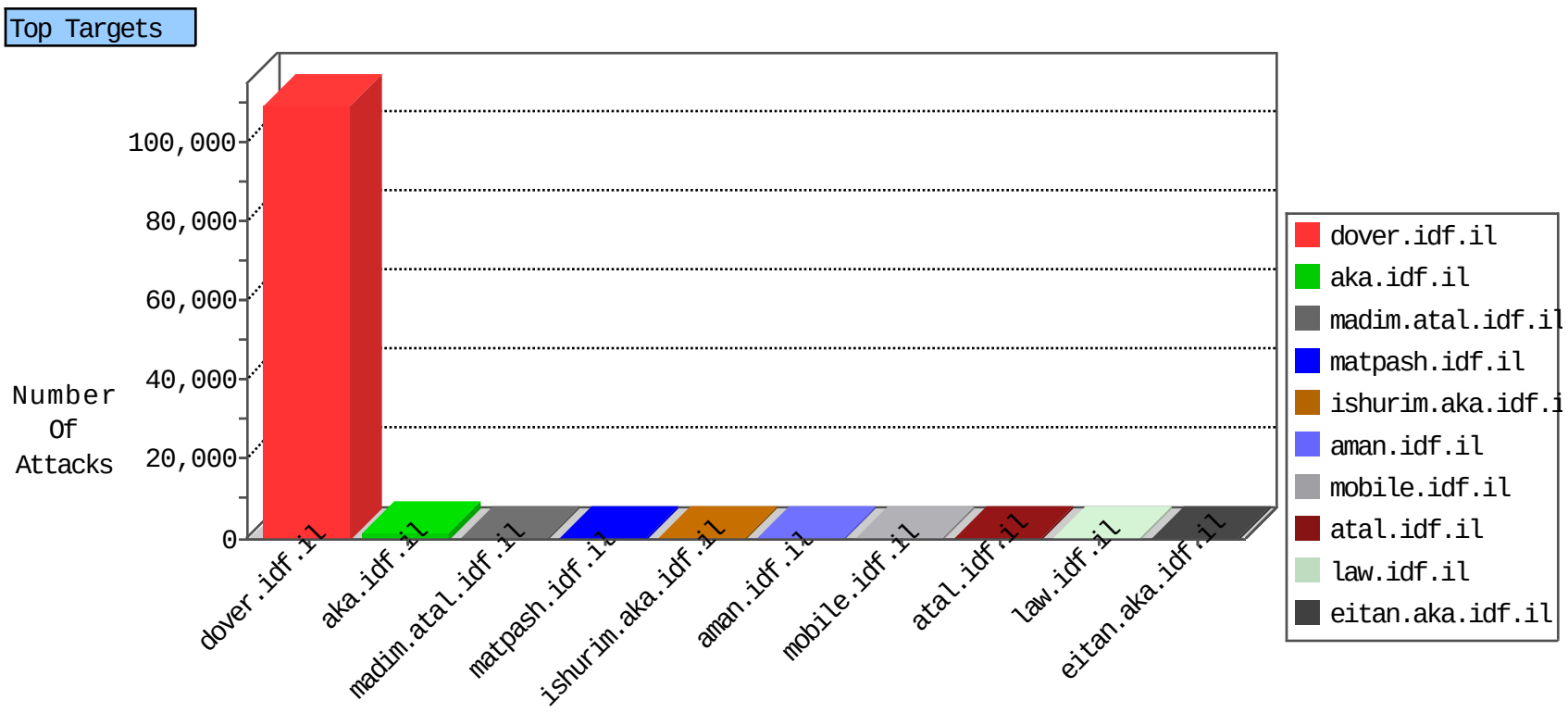
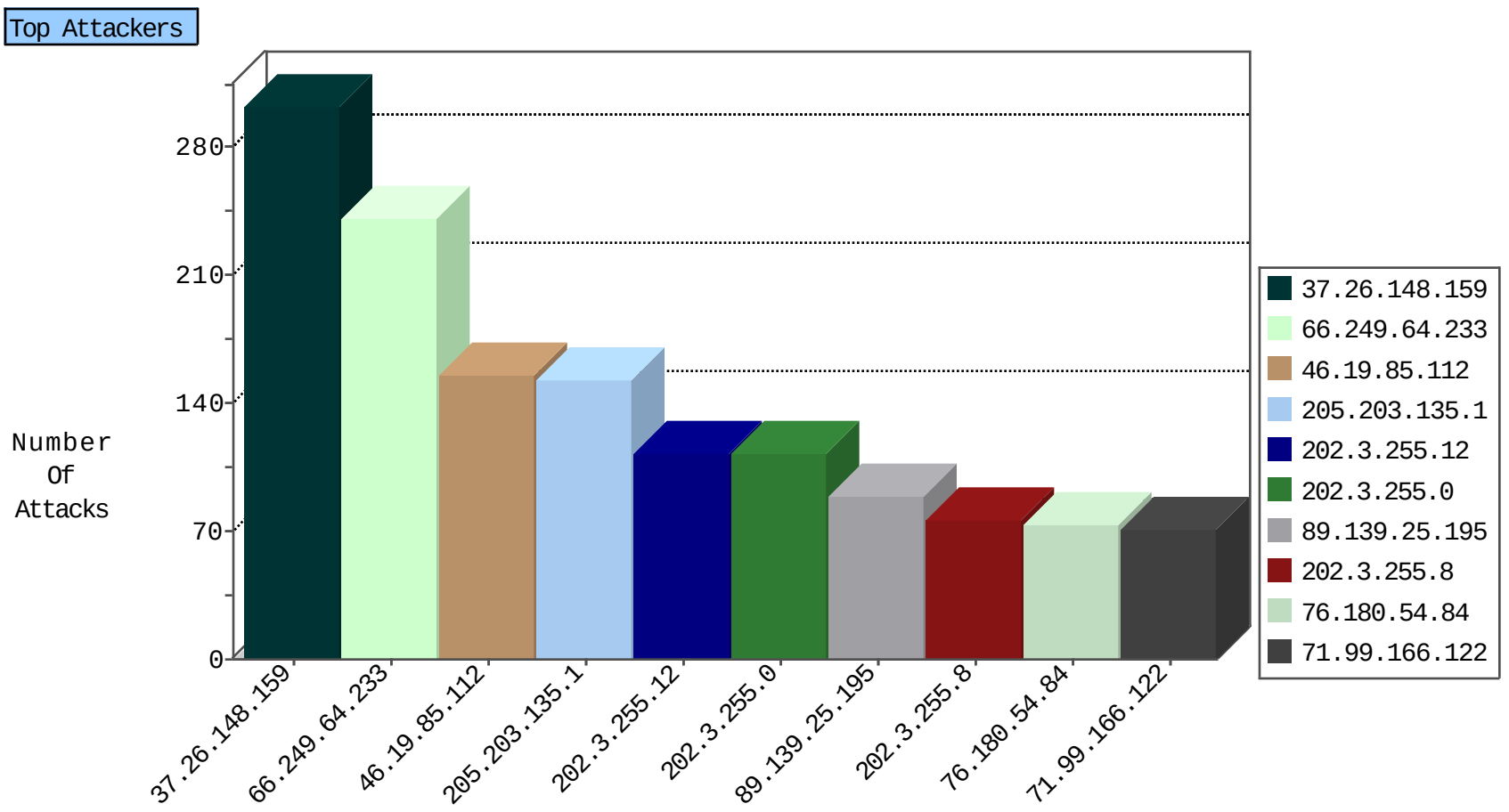
11-12-2015-17:04:03 to 11-12-2015-18:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-12-2015-17:04:03 to 11-12-2015-18:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.69.76	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	6435
183.52.49.111	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3388
83.56.162.60	Spain	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2913
217.64.112.41	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2639
123.201.200.126	India	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2617
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	523
204.93.154.216	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	362
182.221.30.71	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	197
112.236.6.5	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	115
184.252.68.99	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	44
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	23
132.70.66.14	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	22
37.26.148.159	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	15
2.52.185.64	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	13
126.77.134.41	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	11
79.180.167.225	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
125.11.184.85	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
162.255.34.123	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
121.223.148.41	Australia	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
37.46.39.116	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
31.45.74.100	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
83.168.78.125	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
208.104.220.80	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
93.88.97.119	Italy	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
93.88.97.119	Italy	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
83.233.16.82	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
37.60.47.199	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
70.181.107.50	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
208.68.50.43	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
85.64.230.90	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
31.208.87.25	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
83.233.50.16	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
162.252.115.51	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
68.148.175.13	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.144.51.15	Denmark	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
206.248.42.37	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
64.68.247.9	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
93.63.133.112	Italy	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
196.47.172.34	Cote D'Ivoire	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
24.105.220.17	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
130.139.5.73	Netherlands	147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	1
119.2.40.114	Indonesia	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
216.159.72.27	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
58.176.107.21	Hong Kong	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
89.175.42.5	Russian Federation	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
185.63.171.94	Italy	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
178.147.1.34	Greece	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
76.177.77.83	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
105.235.112.105	Cote D'Ivoire	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

11-12-2015-17:04:03 to 11-12-2015-18:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.15.233	France	147.237.72.166	aka.idf.il	C228: HTTP: AhrefBot crawler	Block	8
192.115.248.2	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
89.216.115.6		147.237.77.216	dover.idf.il	17272: HTTP: Suspicious User-Agent (WindowsNT) With No Separating Space	Block	5
85.65.73.203	Israel	147.237.77.216	dover.idf.il	15323: HTTP: User-Agent (MRSPUTNIK)	Block	3
188.165.15.132	France	147.237.77.176	matpash.idf.il	C228: HTTP: AhrefBot crawler	Block	3
188.165.15.233	France	147.237.77.226	www.chamatz.aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1
173.193.157.42	United States	147.237.0.17	m.my-kosher-kravi.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	1

11-12-2015-17:04:03 to 11-12-2015-18:04:03

Top Attackers In IDS

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

11-12-2015-17:04:03 to 11-12-2015-18:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.26.148.159	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	299
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	224
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	153
202.3.255.12	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	112
202.3.255.0	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	112
202.3.255.8	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	75
76.180.54.84	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	72
71.99.166.122	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	71
162.219.230.208	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
2.54.51.11	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
89.139.25.195	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
193.169.70.108	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
104.158.24.21	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
46.19.85.63	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	42
65.181.120.179	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
35.0.127.52	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
202.3.255.7	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
202.3.255.11	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
202.3.255.15	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
94.197.121.232	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
71.191.231.238	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
41.232.96.91	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
24.171.130.104	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
92.241.40.163	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
80.246.130.223	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
188.165.15.130	France	147.237.77.74	law.idf.il	drop	SAM rule	drop	22
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
192.99.12.99	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
54.224.21.23	United States	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	19
89.139.25.195	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
94.244.41.159	Ukraine	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
176.13.1.54	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
54.244.22.103	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
88.162.251.137	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
85.64.88.93	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
46.19.85.13	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
105.99.18.63	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
66.249.64.243	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
46.19.85.1	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
66.249.93.196	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
100.100.16.161		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	14

11-12-2015-17:04:03 to 11-12-2015-18:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	121
2.54.23.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	57
109.64.180.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
176.13.1.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
46.19.85.112	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.112	Block	23
89.139.25.195	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 89.139.25.195	Block	14
80.246.137.52	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
2.54.23.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4
46.19.85.4	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	3
79.182.175.186	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.182.175.186	Block	3
109.65.108.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
31.154.94.11	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
81.218.151.130	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.181.28.187	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
40.77.167.0	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	2
46.117.245.122	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
87.69.32.22	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.171.17	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.27.105.110	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.246.137.52	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
79.179.173.238	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
149.88.61.168	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.69.50	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
107.172.18.16	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22921-ar/dover.aspx)	Block	1
85.64.88.93	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.57.43.67	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.12.145.42	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.230.102.48	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
109.67.158.26	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
46.121.121.92	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
89.139.25.195	Israel	147.237.76.200	eitan.aka.idf.il	Too Many 404: Response Code per Session	Block	1
207.46.13.57	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.57	Block	1
79.180.191.120	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.2.176	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.64.7.85	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.160	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/qiyus/qeneral/default.a	Block	1
85.65.5.105	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.35.19	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.230.102.48	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
131.253.25.191	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
74.10.162.1	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
64.71.32.30	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/test/wp-admin/	Block	1
37.26.148.219	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
207.46.13.82	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-18645- <!-- google_ad_section_end --><div class=	Block	1
84.108.18.80	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.86	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/1132-8613-he/navy.aspx.aspx	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
85.65.140.11	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/sip_storage/files/4/70914.pdfâ€?	Block	1
46.19.85.112	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 46.19.85.112	Block	1

11-12-2015-17:04:03 to 11-12-2015-18:04:03