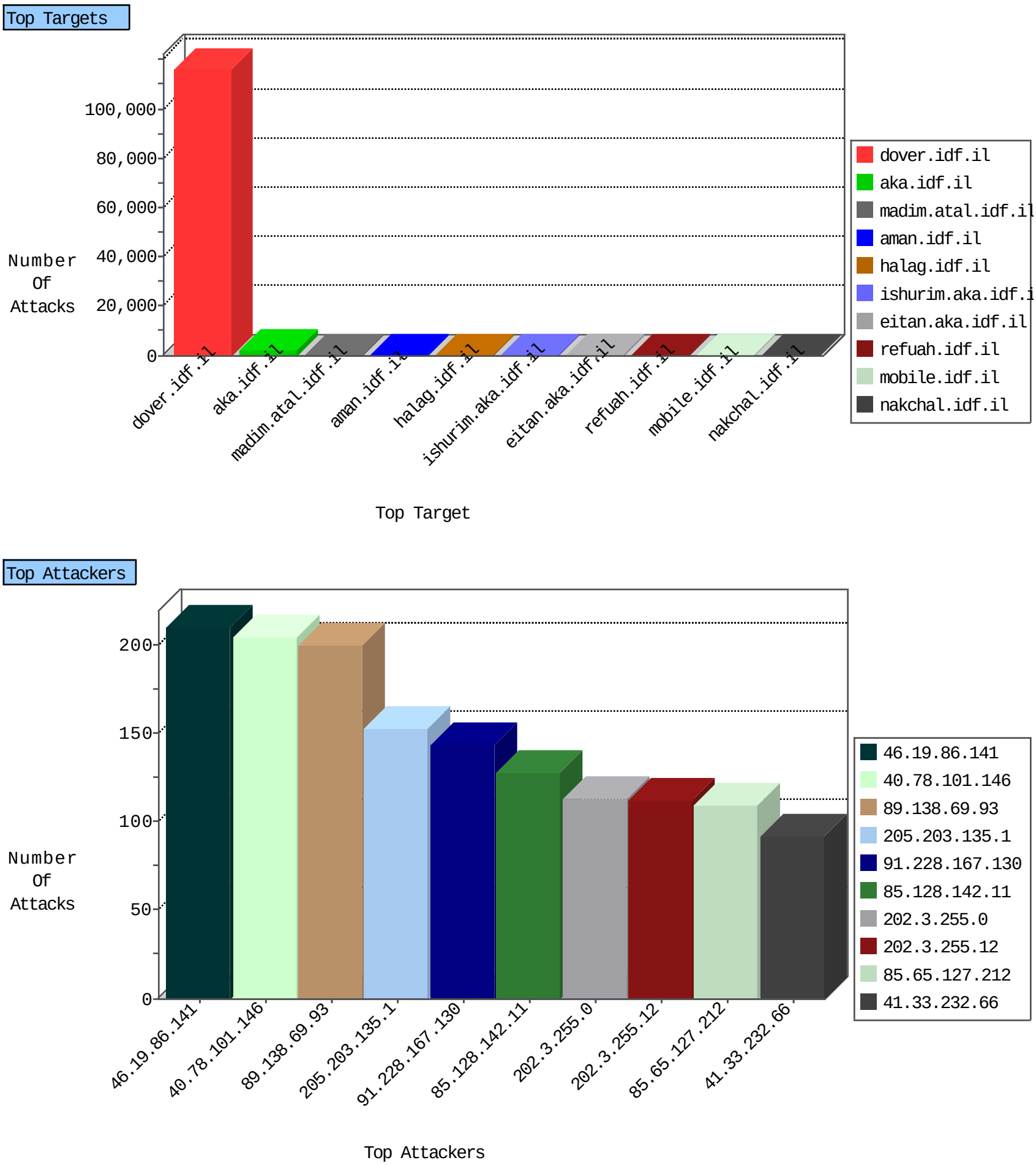
11-12-2015-18:04:06 to 11-12-2015-19:04:06

IDF Under Attack
Daily Report



11-12-2015-18:04:06 to 11-12-2015-19:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
131.165.87.96	Denmark	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2749
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1327
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1240
204.93.154.216	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	171
111.250.236.33	Taiwan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	100
2.52.48.167	Israel	147.237.77.243	mobile.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	61
218.150.192.93	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	56
110.245.90.118	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	47
92.43.67.48	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	40
219.129.187.16	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32
176.12.140.38	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	15
94.244.86.127	Lithuania	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	14
37.142.117.192	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	13
97.68.255.100	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10
176.13.6.31	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
100.100.62.128		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	7
80.74.108.2	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
183.149.28.10	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
81.218.80.110	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
79.181.223.142	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
212.25.121.195	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
74.196.113.75	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
2.143.56.32	Spain	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
212.76.109.229	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
24.152.254.116	United States	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	drop	2
83.233.120.91	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
196.47.176.35	Cote D'Ivoire	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
69.170.220.41	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
107.152.82.27	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
46.9.202.22	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
98.167.196.47	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
24.206.22.62	Bahamas	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
82.209.160.45	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
181.166.185.29	Argentina	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
68.6.99.30	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
65.75.80.106	Bahamas	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
216.45.122.63	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
77.239.152.19	Italy	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
174.138.210.59	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
72.140.108.30	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
135.23.251.80	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
63.248.99.87	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
89.233.196.93	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
209.83.33.7	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
50.78.38.40	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
85.24.163.123	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
198.217.118.70	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

11-12-2015-18:04:06 to 11-12-2015-19:04:06

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
198.190.245.10	United States	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
188.165.15.132	France	147.237.77.176	matpash.idf.il	C228: HTTP: AhrefBot crawler	Block	3
79.176.228.140	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
151.80.31.136	Italy	147.237.76.42	refuah.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.202	France	147.237.76.30	himush.idf.il	C228: HTTP: AhrefBot crawler	Block	1

11-12-2015-18:04:06 to 11-12-2015-19:04:06

Top Attackers In IDS

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

11-12-2015-18:04:06 to 11-12-2015-19:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
40.78.101.146	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	204
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	153
91.228.167.130	Slovakia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	143
85.128.142.11	Poland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	128
202.3.255.0	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	113
202.3.255.12	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	111
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	92
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	92
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
37.140.141.2	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	76
202.3.255.8	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	73
46.253.81.86	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	64
192.115.177.202	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
49.15.219.229	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
197.32.189.88	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
85.65.127.212	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	56
41.223.160.150	Sudan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
85.65.127.212	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	51
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
37.26.146.228	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
202.3.255.11	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
202.3.255.15	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
31.154.94.10	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	37
208.69.40.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
202.3.255.7	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
5.29.97.223	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	37
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
77.125.113.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
79.183.230.68	Israel	147.237.76.31	nakchal.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
188.247.72.217	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
100.100.119.107		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	33
85.130.133.17	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	31
213.57.129.222	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	30
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
84.108.126.157	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	29
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
188.165.15.130	France	147.237.77.74	law.idf.il	drop	SAM rule	drop	27
100.100.109.37		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	27
5.29.175.165	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	26
176.12.151.241	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	26
5.29.175.165	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	26
66.249.64.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
100.100.62.128		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
197.199.171.26	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	24
66.249.64.243	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24

11-12-2015-18:04:06 to 11-12-2015-19:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.138.69.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	128
46.19.86.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	106
46.19.86.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	87
85.64.124.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
89.138.69.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	57
176.13.9.66	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	51
79.176.34.193	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	14
89.138.69.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	14
2.54.23.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
80.246.136.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
2.54.11.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
94.159.203.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.178.79	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.48.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
149.88.53.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	2
85.65.200.220	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.67.48.31	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.176.34.193	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/sip_storage/files/4/	Block	2
2.54.161.15	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
212.227.119.27	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/giyus/main/defaulten.asp	Block	2
46.19.86.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	2
192.99.39.235	Canada	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	2
79.177.189.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m	Block	2
212.227.119.27	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
176.13.19.217	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.23.187	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	2
2.54.130.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.28.172.39	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	1
109.66.149.177	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
46.116.37.245	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
93.173.52.140	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
2.52.51.110	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.182.13.16	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.32.179.49	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.224	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/civiladministration/headayush	Block	1
37.26.148.144	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
117.78.13.57	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/894-he	Block	1
31.154.94.10	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
84.110.33.136	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
2.54.149.76	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.183.185.206	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/default.aspxali	Block	1
207.46.13.149	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5/109335.pdf×³Â¦×³×ŸÂ¿Â½×³Â?-×³×ŸÂ¿Â½×³×ŸÂ¿Â½×³Â¦×³×ŸÂ¿Â½×³×ŸÂ¿Â½	Block	1
46.120.99.199	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
95.86.93.210	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 95.86.93.210	Block	1
79.180.169.46	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
176.13.8.183	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.146.176	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

11-12-2015-18:04:06 to 11-12-2015-19:04:06