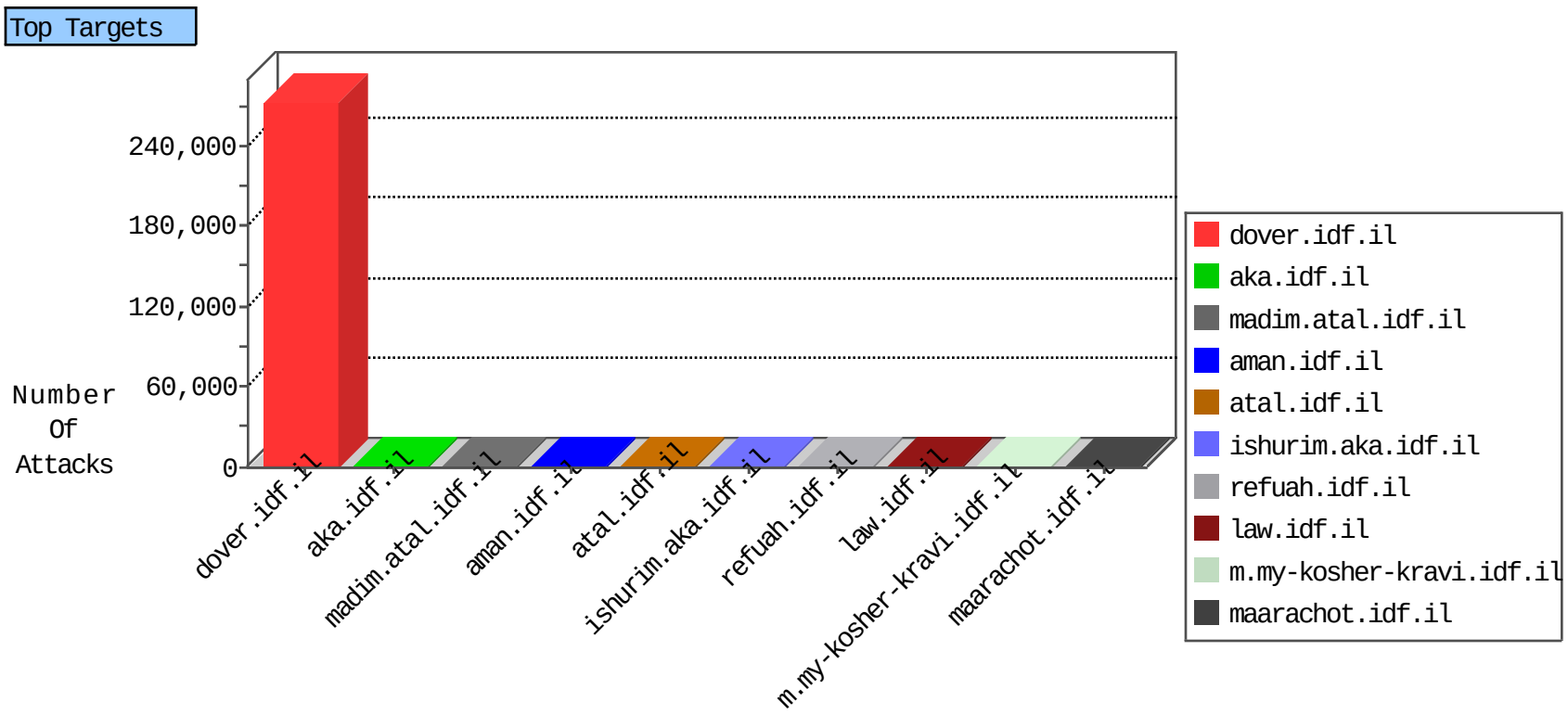
11-20-2015-08:04:09 to 11-20-2015-09:04:09

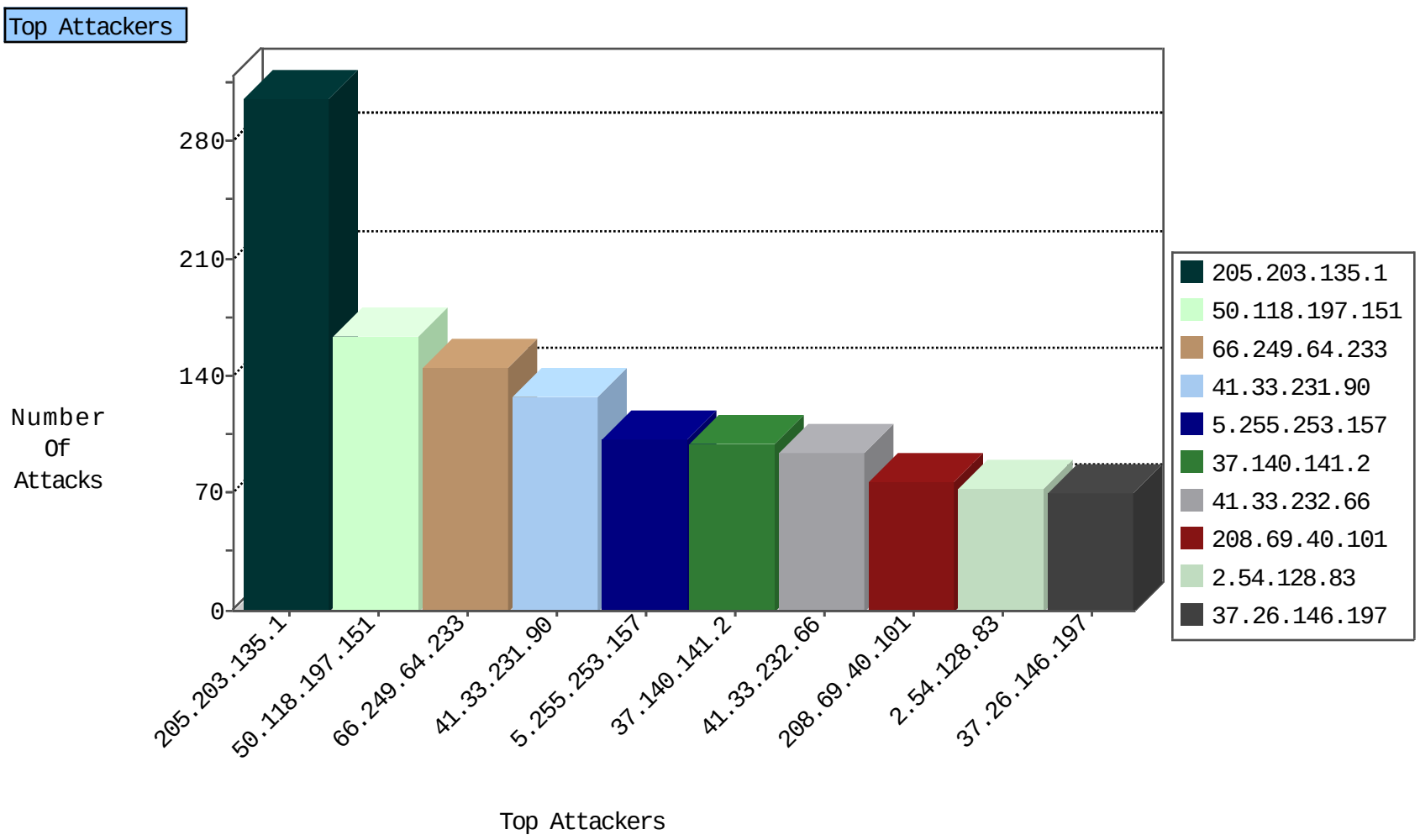
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

11-20-2015-08:04:09 to 11-20-2015-09:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
52.33.66.29	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	522
82.145.218.113	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	13
204.93.154.216	United States	147.237.77.216	dover.idf.il	JLM_Dover_Con_Limit_Https	drop	11
83.233.120.46	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
83.233.115.95	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
64.68.243.103	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
99.66.218.32	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
213.185.249.81	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
222.186.34.204	China	147.237.76.44	e.refuah.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
83.233.133.34	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
193.12.174.80	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
69.9.76.15	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
104.245.224.80		147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
66.129.62.127	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.135.253.75	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
213.148.7.110	Russian Federation	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
82.164.21.30	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
180.97.106.36	China	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
81.191.73.101	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
167.216.16.38	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
62.72.247.24	Finland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
89.176.164.70	Czech Republic	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
209.159.197.52	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
24.105.238.119	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
87.245.167.106	Russian Federation	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
206.174.247.100	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
74.205.152.12	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
142.4.193.203	United States	147.237.76.38	e.e.meitav.idf.i	Block_Udp_All_Nets	drop	1
69.196.155.21	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
118.5.50.62	Japan	147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	1
84.208.242.34	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
196.47.173.15	Cote D'Ivoire	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
188.175.155.90	Czech Republic	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
67.22.82.4	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
98.27.208.103	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
216.238.242.98	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
212.50.4.119	Bulgaria	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
174.138.202.101	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
93.185.1.39	Czech Republic	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
45.124.216.2		147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
89.160.31.37	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
208.111.72.43	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
78.136.77.77	Spain	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
152.3.208.12	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
73.133.69.12	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
141.32.80.34	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
87.72.115.57	Denmark	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
198.111.33.13	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
83.233.133.70	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
193.34.68.7	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

11-20-2015-08:04:09 to 11-20-2015-09:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.165.129	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3

11-20-2015-08:04:09 to 11-20-2015-09:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.3.255.8	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	28
202.3.255.12	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	28
94.130.205.63	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
213.57.58.162	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.78.154.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
148.248.0.33	147.237.77.216	Mexico	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.131.47.17	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.130.163.75	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
199.34.191.33	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.248.233.31	147.237.77.216	Mexico	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.135.9.84	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

11-20-2015-08:04:09 to 11-20-2015-09:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
205.203.135.1	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	306
50.118.197.151	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	156
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	102
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	102
37.140.141.2	Russian Federation	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	100
66.249.64.233	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	96
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	94
208.69.40.101	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	77
37.26.146.197	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	70
80.181.120.2	Italy	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	68
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	64
54.224.21.23	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	63
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	63
72.9.148.10	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	58
218.249.201.130	China	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	57
109.200.30.168	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	48
37.26.148.156	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	42
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	41
66.249.93.200	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	41
37.201.168.140	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	40
195.34.150.18	Austria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	39
202.3.255.12	French Polynesia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	38
41.202.219.73	Cameroon	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	38
66.249.64.243	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	37
202.3.255.8	French Polynesia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	37
108.59.253.71	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
66.249.64.233	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
79.66.252.209	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	34
52.34.23.129	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	34
52.11.255.218	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	33
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	33
46.19.85.141	Israel	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
66.249.93.192	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	30
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	29
54.244.22.103	United States	147.237.77.216	dover.idf.i	Bad TCP sequence	Invalid ACK number	monitor	27
54.244.22.103	United States	147.237.77.216	dover.idf.i	Bad TCP sequence	Invalid ACK number	alert	25
66.249.64.238	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop		drop	24
204.12.251.37	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
190.33.50.47	Panama	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
136.243.5.203	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
199.255.211.74	Anonymous Proxy	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
149.78.181.107	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
66.249.93.196	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
87.203.103.152	Greece	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
169.253.194.1	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
207.46.13.130	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.86.78	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
37.26.146.218	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.128.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	49
176.12.148.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
193.106.54.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
176.12.146.203	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	6
37.26.146.140	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	4
176.13.9.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.118.155.216	Ukraine	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
176.13.14.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.149.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.16.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.37.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.57.184.121	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.23.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.65.24.79	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ufi/reaction/	Block	2
176.13.2.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.176.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.2.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.52.35.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.142.68.118	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.188.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.12.138.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
93.172.140.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
207.241.226.42	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.241.226.42	Block	2
176.13.22.104	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
5.29.178.252	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
104.131.25.244	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/894-he/nakhal.aspxshared/usercontrols/headerupper/	Block	1
204.93.154.216	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.120.81.88	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.4.199	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 176.13.4.199	None	1
37.26.147.220	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.54.63.34	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
147.235.8.74	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
84.109.73.58	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.253	Israel	147.237.77.176	matpash.idf.il	Parameter Type Violation searchText in www.cogat.idf.il/901-he/cogat.aspx	Block	1
31.154.182.48	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
207.46.13.100	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/	Block	1
66.249.64.157	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/size100x0/3261.jpg	Block	1
37.26.148.173	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.36	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
84.111.241.139	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.23.210	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/mobile/login.aspx	Block	1
31.154.182.48	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
109.65.121.210	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.130	United States	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
173.252.120.119	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.64.135.226	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.118.155.216	Ukraine	147.237.77.74	law.idf.il	PHP Attempt	Block	1
31.168.13.78	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.67.27.183	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1