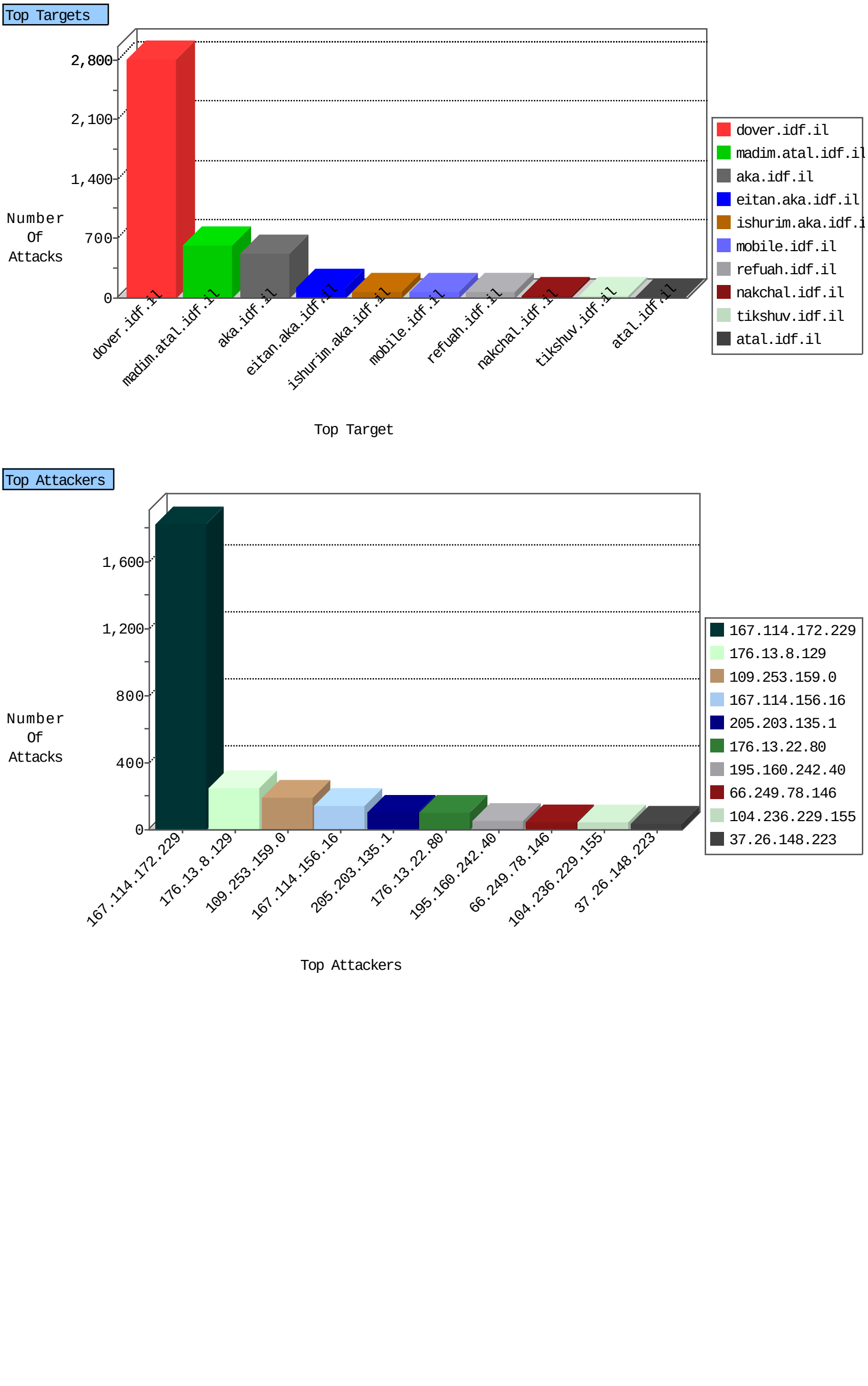
05-01-2016-10:04:02 to 05-01-2016-11:04:02

IDF Under Attack Daily Report



05-01-2016-10:04:02 to 05-01-2016-11:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	7540
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2669
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	44
79.183.99.232	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
212.235.98.139	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
2.53.38.114	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
82.81.12.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
199.203.215.1	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
147.236.238.250	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
74.50.178.222	Canada	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	2
120.132.50.135	China	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	drop	2

05-01-2016-10:04:02 to 05-01-2016-11:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

05-01-2016-10:04:02 to 05-01-2016-11:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
113.240.250.154	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
46.116.34.227	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.65.115.171	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.178	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.189.26.18	147.237.0.17	Austria	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.148.201	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.151.43.108	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.69.16.90	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.199.81	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.181.205	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.203.151.133	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.39.226	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.136.10	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.0.124	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.216.41	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
113.240.250.154	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
62.219.160.66	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.65.188.18	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.133	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.189.26.18	147.237.0.33	Austria	idf.il	ET SCAN NMAP -sS window 1024	1
37.26.149.128	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
217.69.133.242	147.237.72.166	Russian Federation	aka.idf.il	portscan: TCP Distributed Portscan	1
87.69.249.140	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.193	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.28.34	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.144.180	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.36.185	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.150.249.181	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.93.159	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.160.242.40	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.137.137	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
187.188.72.11	147.237.77.178	Mexico	e.matpash.idf.il	ET SCAN NMAP -sS window 3072	1
79.182.8.109	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.50.46.232	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
71.117.155.69	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 4096	1

05-01-2016-10:04:02 to 05-01-2016-11:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.172.229	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1827
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	102
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
195.160.242.40	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	46
104.236.229.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
37.26.148.223	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
81.218.251.252	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
37.26.148.228	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
212.179.155.129	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
198.208.27.69	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
87.203.102.200	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
176.13.15.239	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
37.26.149.220	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
37.26.146.150	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	21
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
77.125.75.80	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
205.167.7.245	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
62.90.139.244	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
207.46.13.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
89.138.62.157	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
80.178.157.42	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
109.253.224.83	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
50.116.30.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.21.23	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.106.46.74	Palestinian Territory, Occupied	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.114	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.115	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
149.78.249.63	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.53.153.98	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.148.201	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
185.89.217.226	Netherlands	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
66.249.93.119	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
185.89.217.232	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
185.89.217.233	Netherlands	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.22.129.253	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.89.217.234	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.13.5.150	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.148.202	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
31.154.248.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.8.129	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	251
109.253.159.0	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	191
176.13.22.80	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	99
109.253.204.23	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/login parameter Password	Block	28
2.53.142.31	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
176.13.9.152	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
109.253.224.127	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
109.253.221.43	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
109.253.224.125	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
80.246.133.64	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
37.46.38.90	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	5
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	4
109.253.201.70	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter NewPassword	Block	4
185.89.217.225	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
109.253.213.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.224.84	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.134.76	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter NewPassword	Block	3
109.253.136.212	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
212.179.33.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/	Block	3
109.253.224.120	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.144.18	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.201	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	2
194.90.99.193	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.90.99.193	Block	2
109.253.224.124	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal	Block	2
157.55.39.53	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.85.131	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.55.29.111	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.160	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
212.179.33.2	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	2
109.253.224.115	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam/asp/index.asp	Block	1
37.46.38.90	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 37.46.38.90	Block	1
81.218.56.171	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 81.218.56.171	Block	1
2.53.59.212	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
141.212.122.113	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to /x	Block	1
77.125.75.80	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
217.69.133.245	Russian Federation	147.237.72.166	aka.idf.il	Unknown Parameter fb709480 in aka.idf.il/giyus/	None	1
46.19.85.10	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
80.246.133.34	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
31.168.118.94	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
66.249.79.167	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
46.19.85.238	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
37.46.38.90	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/8/	Block	1
185.89.217.228	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.178.242.183	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	1