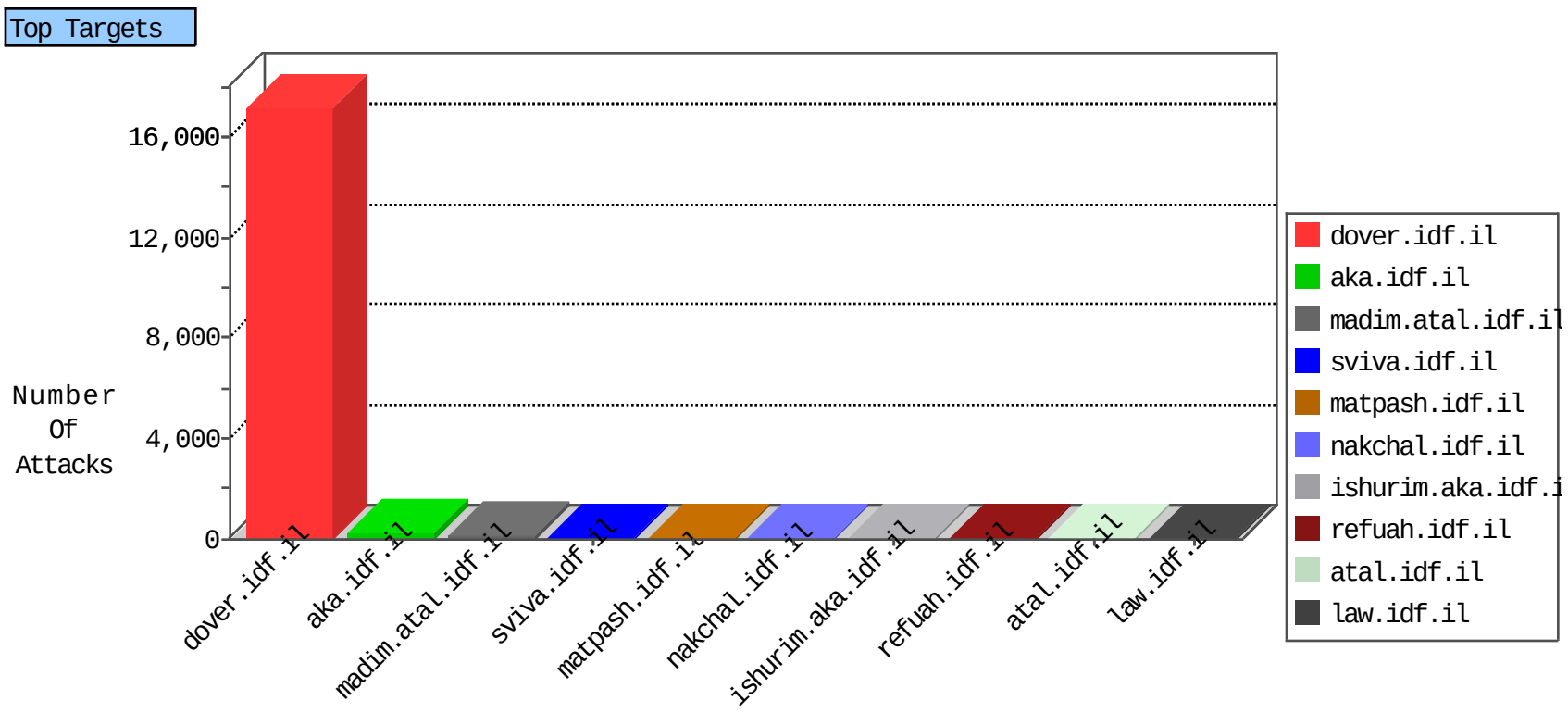
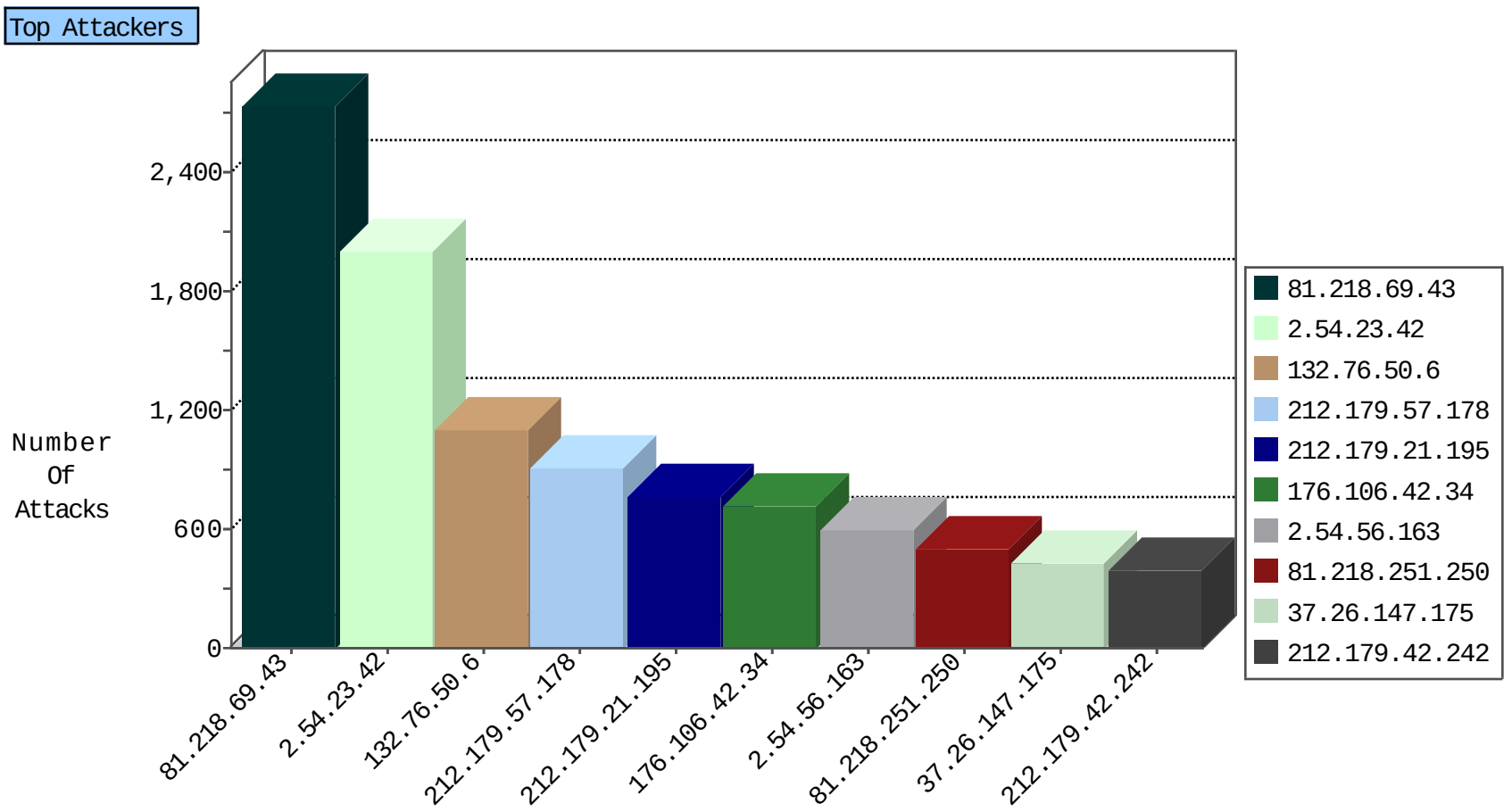
04-19-2015-09:03:01 to 04-19-2015-10:03:01

IDF Under Attack
04-19-2015-09:03:01

Top Targets



Top Attackers



04-19-2015-09:03:01 to 04-19-2015-10:03:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.67.32	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3751
192.115.116.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	94
149.78.84.105	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	69
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	36
109.65.105.42	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	19
109.64.166.242	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
85.250.100.172	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	15
66.249.93.238	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
212.179.42.66	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
212.179.177.163	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
79.182.126.103	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
66.249.93.241	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
134.147.203.115	Germany	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	2
121.32.2.196	China	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	2
77.127.239.206	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
185.32.179.183	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
219.74.36.219	Singapore	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
80.246.139.17	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
46.19.85.253	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
209.88.198.1	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
109.253.131.229	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
71.6.165.200	United States	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
5.29.124.51	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
37.26.146.168	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
124.232.142.220	China	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
46.19.85.30	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

04-19-2015-09:03:01 to 04-19-2015-10:03:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
138.134.102.16	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
46.19.85.150	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
138.134.102.15	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
37.26.146.199	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
212.179.61.125	Israel	147.237.77.235	sviva.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
81.218.188.139	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
176.106.46.74	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
82.102.169.113	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.19.86.208	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
192.115.90.82	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.120.27.62	Romania	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.53	Israel	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.70.114	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
62.90.35.105	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
198.20.69.98	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
94.159.230.224	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
80.179.39.12	Israel	147.237.77.216	dover.idf.il	C1000122: HTTP: Access to - .exe or .dll	Permit	1
46.19.85.169	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
212.179.21.195	Israel	147.237.77.235	sviva.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
188.138.9.50	Germany	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
46.19.86.204	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
188.138.9.50	Germany	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1

04-19-2015-09:03:01 to 04-19-2015-10:03:01

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
81.218.118.124	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	2
78.146.64.180	United Kingdom	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.45.175	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	1
94.159.189.85	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.186.27	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.65.127	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.208	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
212.76.99.24	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
176.12.141.11	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.201.208	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1

04-19-2015-09:03:01 to 04-19-2015-10:03:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
81.218.69.43	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2743
2.54.23.42	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2001
132.76.50.6	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1108
212.179.57.178	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	905
212.179.21.195	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	727
176.106.42.34	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	711
2.54.56.163	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	601
81.218.251.250	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	499
37.26.147.175	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	427
212.179.42.242	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	387
2.54.5.200	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	298
212.179.159.253	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	256
212.179.132.202	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	120
212.179.177.148	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	82
66.249.93.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	81
109.65.108.24	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	78
46.19.85.202	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	76
84.108.155.44	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	71
37.26.147.206	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	67
80.230.125.142	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	64
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	63
212.179.177.163	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	58
212.25.103.10	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	57
37.26.146.142	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	56
212.179.61.125	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	55
66.249.93.160	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	53
173.32.32.79	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	50
199.203.215.1	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	50
176.12.150.222	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	49
192.116.127.113	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	48
46.19.85.34	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	48
111.93.130.83	India	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	44
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	43
212.199.247.70	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	43
176.12.142.149	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	41
109.253.158.14	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	40
176.12.141.11	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	40
176.12.145.116	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	40
194.54.168.76	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	40
84.94.103.119	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	38
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	38
212.179.21.195	Israel	147.237.77.235	sviva.idf.i	First packet isn't SYN	drop	drop	38
66.249.78.173	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	38
212.150.214.122	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	38
176.12.142.163	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	38
176.12.142.61	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	38
138.134.102.15	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	38
176.12.140.29	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
192.117.134.156	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
176.12.138.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	94
2.54.150.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	28
2.54.19.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	21
77.127.224.85	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	11
109.67.52.72	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	9
2.52.145.197	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.52.145.197	Block	5
93.172.136.64	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	4
79.182.63.180	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	3
94.153.66.163	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-11442-en/	Block	3
80.246.133.183	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	3
37.26.148.154	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 37.26.148.154	Block	3
46.116.21.57	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	3
212.143.3.44	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	2
207.46.13.10	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
81.218.188.139	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	2
2.52.145.216	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	2
66.249.73.211	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	2
192.117.134.124	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.52.137.164	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Unknown Parameter pageNum in www.aka.idf.il/patzar/klali/default.asp	None	1
66.249.64.63	Israel	147.237.72.166	aka.idf.il	Unknown Parameter list in www.aka.idf.il/megurim/news/	None	1
37.26.148.171	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.35	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-13437-he/dover.aspx×³Ö³Æ’Ö¶â€™Ö³â€šÖ²Â¯Ö³Æ’×’â,¬ÂšÖ³â€šÖ²Â¿Ö³Æ’×’â,¬ÂšÖ³â€šÖ²Â½×³Â?×³Ö³Æ’Ö¶â€™Ö³â€šÖ²Â¯Ö³Æ’×’â,¬ÂšÖ³â€šÖ²Â¿Ö³Æ’×’â,¬ÂšÖ³â€šÖ²Â½×³Ö³Æ’Ö¶â€™Ö³â€šÖ²Â¯Ö³Æ’×’â,¬ÂšÖ³â€šÖ²Â¿Ö³Æ’×’â,¬ÂšÖ³â€šÖ²Â½×³Â£	Block	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
2.52.146.69	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
66.249.73.213	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/938-he/hamaz.aspx	Block	1
84.110.54.47	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
58.22.150.79	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/rights/asp/info.asp/trackback/	Block	1
212.179.21.195	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
80.246.130.87	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
2.54.190.19	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
192.117.134.124	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/yiyus	Block	1
2.52.138.152	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	1
95.86.116.178	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
66.249.65.178	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
37.142.198.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
212.117.136.8	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/smalim/scriptresource.axd	None	1
82.102.136.69	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
79.178.21.98	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1560	Block	1
176.12.139.238	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
66.249.73.219	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
109.253.139.131	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.250.240.47	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
66.199.231.242	United States	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/brothers/skira/	None	1
213.57.254.23	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
80.246.130.229	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/kapatz/citizencontact.aspx	None	1
37.26.146.187	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1