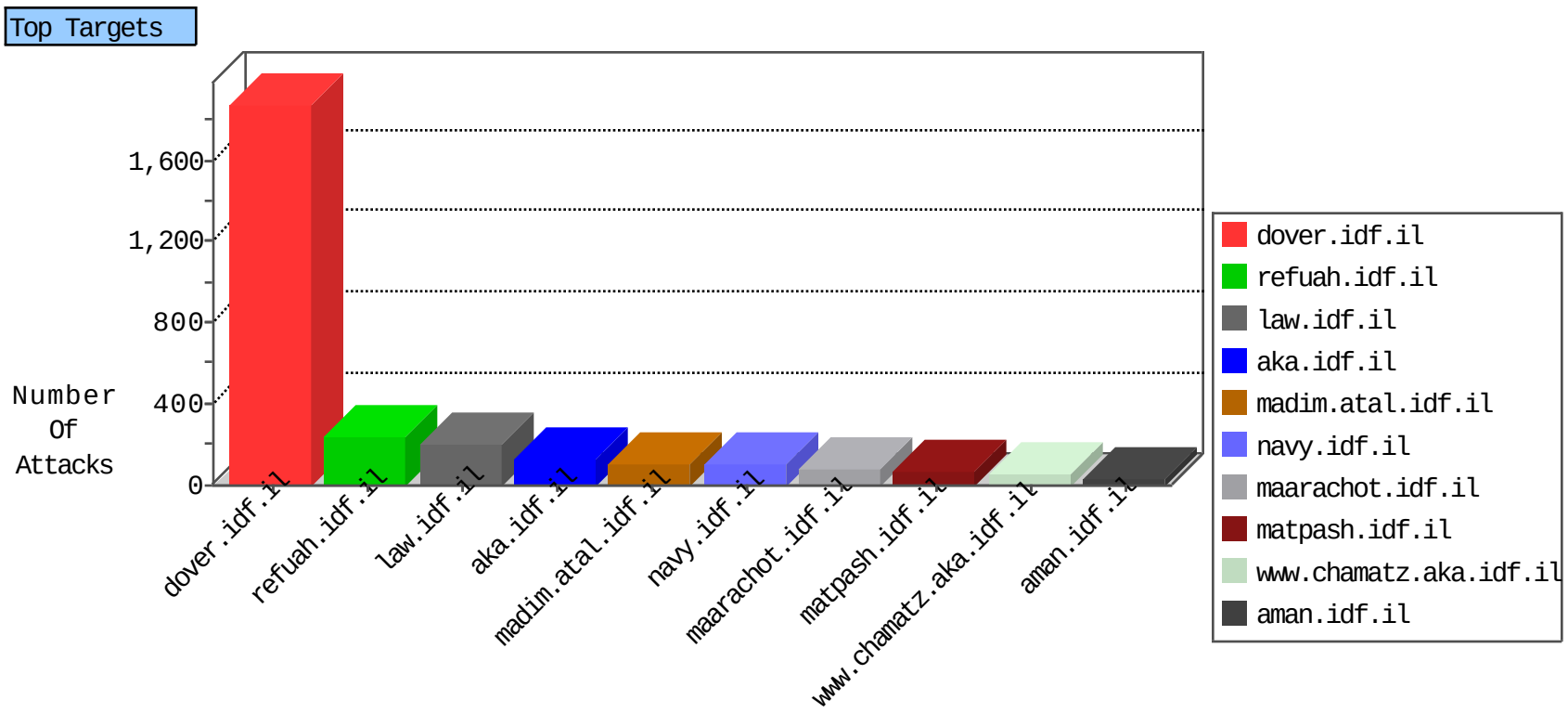
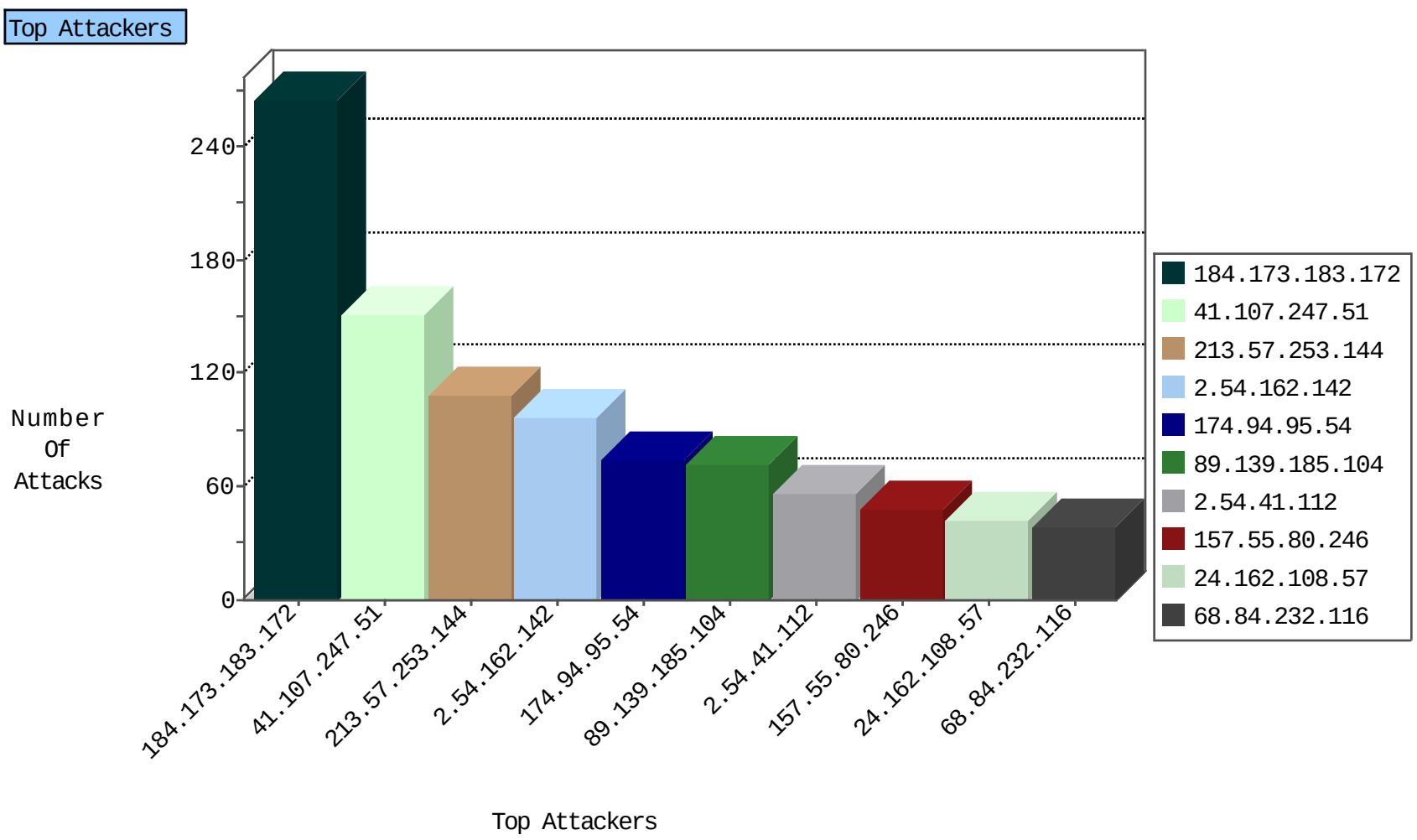
04-11-2015-22:03:08 to 04-11-2015-23:03:08

IDF Under Attack
04-11-2015-22:03:08





04-11-2015-22:03:08 to 04-11-2015-23:03:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
84.110.60.143	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	172
79.129.161.74	Greece	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	64
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	33
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	31
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	30
66.249.64.132	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	29
66.249.64.146	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	26
66.249.83.188	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	24
66.249.83.182	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	23
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	22
66.249.64.150	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	22
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	21
66.249.64.136	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	21
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	21
66.249.78.197	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	20
66.249.83.194	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	17
66.249.78.204	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	17
66.249.78.190	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	16
66.249.67.108	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	15
66.249.64.128	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	14
66.249.67.147	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	12
66.249.67.76	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	12
66.249.93.242	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	12
66.249.65.200	United States	147.237.0.19	madim.atal.idf.il	Block_Ip_Web_In	drop	11
66.249.67.155	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	11
66.249.64.154	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	11
66.249.80.83	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	11
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	11
89.139.185.104	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10
66.249.67.84	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	10
66.249.67.116	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	10
66.249.67.92	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	10
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	9
74.36.143.100	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
66.249.93.239	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	8
66.249.67.100	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	7
66.249.67.3	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	7
66.249.78.160	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	7
66.249.69.101	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	5
66.249.64.41	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	5
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	5
66.249.64.49	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	5
66.249.78.174	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	5
66.249.69.42	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	5
66.249.78.86	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	5
66.249.93.213	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	4
66.249.69.50	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	4
66.249.78.120	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	4
66.249.81.212	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4
66.249.64.120	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	4

04-11-2015-22:03:08 to 04-11-2015-23:03:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	136
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	129
109.67.193.121	Israel	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	10
213.57.253.144	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
218.241.153.80	China	147.237.8.24	e.lifestyle.idf.i	DVRep_B-N_60_100	Block	2
89.139.185.104	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
93.120.27.62	Romania	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
84.228.137.4	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.64.80.33	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.120.27.62	Romania	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
212.199.156.81	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
79.181.59.229	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

04-11-2015-22:03:08 to 04-11-2015-23:03:08

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	4
118.69.174.89	Vietnam	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
58.20.54.249	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
218.241.153.80	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
58.20.54.249	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
218.241.153.80	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 2048	1
218.241.153.80	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -f -sS	1

04-11-2015-22:03:08 to 04-11-2015-23:03:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
41.107.247.51	Algeria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	151
213.57.253.144	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	102
174.94.95.54	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	74
89.139.185.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	69
2.54.41.112	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	56
157.55.80.246	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	48
24.162.108.57	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
68.84.232.116	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
77.127.66.80	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
94.123.204.203	Turkey	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
105.94.25.53	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
212.116.177.130	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
109.253.135.242	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
92.22.141.234	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
93.172.157.16	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
46.121.252.22	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
176.228.165.10	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
176.12.139.193	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
212.76.127.212	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
109.253.145.71	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
85.65.12.249	Israel	147.237.0.34	tikshuv.idf.i	Invalid ACK number	Bad TCP sequence	monitor	20
95.86.87.154	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
46.116.37.153	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
82.80.60.1	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
84.228.137.4	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	16
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
46.19.85.243	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
84.94.165.212	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
157.55.39.42	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
79.129.161.74	Greece	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
157.55.39.6	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
37.26.148.242	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
84.228.56.130	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
85.64.144.138	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
81.218.251.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
70.187.11.243	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
84.229.155.233	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
96.247.49.223	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
79.183.186.121	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
84.228.144.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
176.12.147.240	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
157.55.39.114	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
2.54.162.142	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.162.142	Block	95
109.64.118.246	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	5
80.178.194.206	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 80.178.194.206	Block	4
109.65.132.133	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	3
77.127.32.23	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
84.111.118.6	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 84.111.118.6	Block	3
84.108.96.164	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	3
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
212.199.57.200	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
109.64.118.90	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.65.148.200	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1513	Block	2
109.160.217.207	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
109.160.225.242	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
207.46.13.82	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.82	Block	1
2.54.162.142	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
84.228.137.4	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//webresource.axd	Block	1
79.181.60.109	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.171	United States	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
37.26.148.242	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
95.86.127.241	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/faqselection.aspx	None	1
84.111.115.186	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
109.65.148.200	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 109.65.148.200	Block	1
84.229.29.109	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
167.114.64.100	United States	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
46.19.86.28	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
77.127.147.78	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/rights/asp/info.asp	None	1
213.57.253.144	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
2.54.167.140	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.64.119.92	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
80.178.194.206	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-13518-he/dover.aspx17.10.11×œ	Block	1
46.117.83.50	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
176.12.138.45	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.111.118.6	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/general/6_s3_	Block	1
79.178.130.184	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
5.102.219.81	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
93.173.41.233	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/june/mazen.stm	Block	1
199.203.111.199	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.54.36.80	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
109.65.55.41	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.228.14.19	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233//1134-he/atal.aspx	Block	1
79.180.78.246	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/clientscripØ§Ù„Ù…Ù^Ù, Ø¹ Ø§Ù„Ø±Ø³Ù…Ù…Š, Ø§Ù„Ø¬Ù…Ø´ Ø§Ù„Ø©Ø³Ø±Ø§Ø¦Ù„Ù„Ù, Ø¨Ù†Ù†Š Ø°Ø§Ù†Ø³, Ø§Ù?Š®Ø§Š Ø§Ø¯Ø±Ø¹Ù Š	Block	1
5.255.253.99	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/1/1381.pdf	Block	1
95.86.85.68	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
84.110.77.184	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1