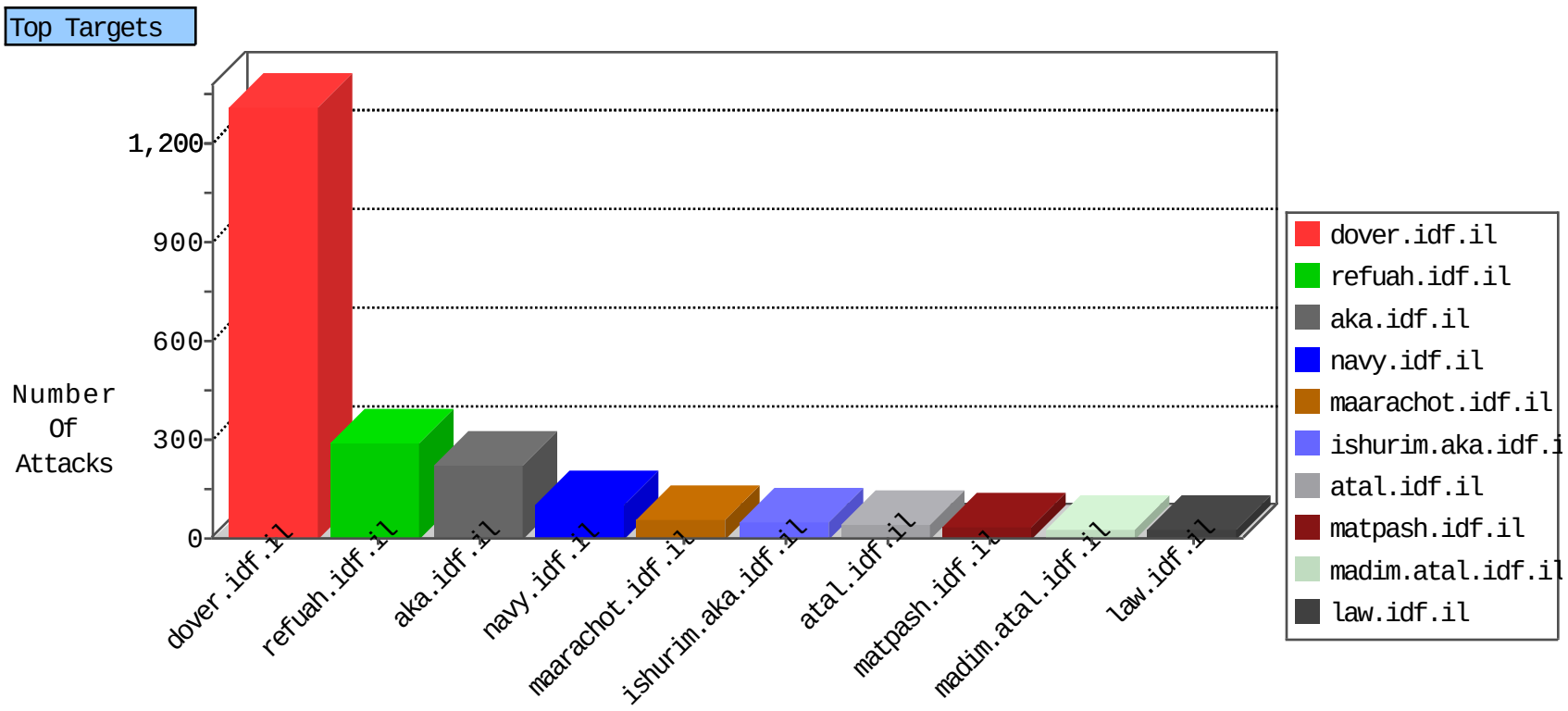
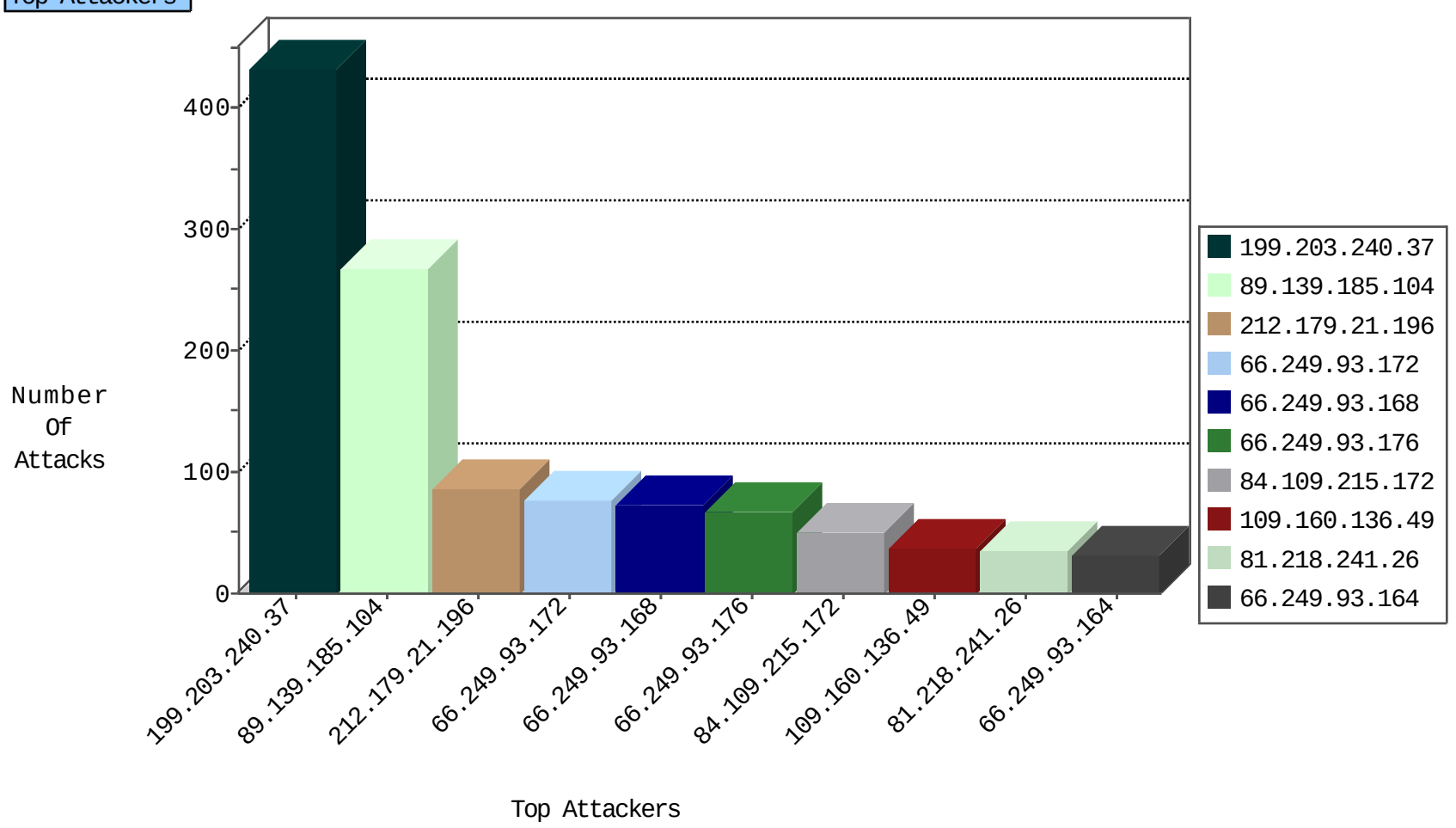
04-12-2015-08:03:00 to 04-12-2015-09:03:00

IDF Under Attack
04-12-2015-08:03:00

Top Targets



Top Attackers



04-12-2015-08:03:00 to 04-12-2015-09:03:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
5.41.84.241	Romania	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1365
195.154.233.184	France	147.237.72.14	dover.idf.il(old)	TCP handshake violation, first packet not syn	drop	892
206.45.162.159	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	678
109.253.144.87	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	667
89.139.185.104	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	615
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	287
213.57.156.128	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	225
192.114.2.36	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	108
194.90.128.25	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	102
66.249.93.172	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	76
66.249.93.168	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	67
66.249.93.176	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	67
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	32
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	30
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	30
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	26
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	25
66.249.64.132	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	24
66.249.93.242	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	24
66.249.93.239	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	18
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	17
66.249.93.245	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	16
66.249.64.136	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	16
66.249.78.28	United States	147.237.76.42	refuah.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
66.249.78.86	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	12
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	12
66.249.69.101	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	11
66.249.78.197	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	11
66.249.67.3	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	10
66.249.78.190	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	10
66.249.67.125	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	10
66.249.64.154	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	9
66.249.69.42	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	9
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	8
66.249.78.60	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	7
66.249.78.174	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	7
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	7
66.249.67.133	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	7
66.249.65.200	United States	147.237.0.19	madim.atal.idf.il	Block_Ip_Web_In	drop	6
66.249.67.100	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	6
66.249.67.84	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	6
66.249.67.76	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	5
66.249.78.248	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	5
66.249.69.50	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	5
66.249.78.67	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	5
66.249.67.92	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	5
66.249.69.34	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	5
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5

04-12-2015-08:03:00 to 04-12-2015-09:03:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
89.139.185.104	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
2.54.20.12	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
203.213.121.100	Australia	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
79.180.2.131	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.65.5.248	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
94.159.157.236	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

04-12-2015-08:03:00 to 04-12-2015-09:03:00

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
109.253.130.120	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.65	China	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	1
61.240.144.66	China	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
2.52.149.194	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1

04-12-2015-08:03:00 to 04-12-2015-09:03:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
199.203.240.37	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	432
89.139.185.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	262
212.179.21.196	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	87
84.109.215.172	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	51
109.160.136.49	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
79.183.132.172	Israel	147.237.77.243	mobile.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
192.116.177.210	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
37.26.148.168	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
213.57.247.65	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
79.177.128.26	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
109.160.200.98	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
46.19.85.119	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
208.99.238.226	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
80.215.194.45	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
109.253.128.42	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
91.232.100.14	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
176.12.151.215	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
84.109.18.75	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
31.168.137.82	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
192.0.86.147	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
77.230.182.33	Spain	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
101.163.2.185	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
109.64.157.188	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
212.179.143.34	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
37.26.147.186	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
192.117.138.210	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
37.26.147.203	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
2.52.147.231	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
188.248.208.200	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
203.213.121.100	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
84.228.144.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
207.46.13.82	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
157.55.39.6	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
85.154.56.17	Oman	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
62.90.215.152	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
212.235.83.207	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
5.102.254.191	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
79.180.25.90	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
101.163.2.185	Australia	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	2
46.19.86.11	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
2.54.0.52	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
213.8.129.145	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.116.146.30	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
94.188.248.67	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
87.68.145.10	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	26
2.54.150.227	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.150.227	Block	23
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
95.86.116.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
84.108.171.194	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	2
82.80.62.56	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
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
88.203.16.129	Malta	147.237.76.30	himush.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
82.166.221.34	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/tfasim.aspx	None	1
79.176.115.132	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
195.78.33.120	Croatia	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	1
132.70.157.117	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
87.68.145.10	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/homas/site/homasformphase4.aspx	None	1
206.225.87.63	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
82.80.42.83	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
157.55.39.55	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	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
88.203.16.129	Malta	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
79.177.22.110	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
195.78.33.120	Croatia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
138.134.192.10	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	1
37.26.147.203	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
87.68.145.10	Israel	147.237.72.166	aka.idf.il	Unknown Parameter count in www.aka.idf.il/homas/site/resources/services/wsmaterials.asmx/getmaterialpossiblenamesbynamestart	None	1
212.143.3.44	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
82.80.62.56	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim/templates/www.behazdaa.org.il	Block	1
66.199.231.242	United States	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/brothers/faq/	None	1
91.231.193.150	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
84.109.14.215	Israel	147.237.77.216	dover.idf.il	NULL Character in Method	Block	1
80.178.173.21	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	1
197.89.168.192		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/homefront/homefront3.stm	Block	1
147.236.238.70	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/registrationwizard/step3.aspx	None	1
46.117.130.235	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
87.68.159.224	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 87.68.159.224	Block	1
212.179.161.238	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/home.aspx	None	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	1
176.12.142.182	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
85.65.182.125	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
80.246.130.12	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
199.203.240.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/promotioncube/	Block	1
149.78.71.218	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
61.135.190.200	China	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to 147.237.0.15/	Block	1
87.68.159.224	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	1
176.12.147.67	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.54.150.227	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
112.111.188.90	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/brothers/skira/default.asp/trackback/	Block	1
206.225.87.63	United States	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1
80.246.130.175	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
149.78.253.190	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
62.210.114.129	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/8/3198.pdf/trackback/	Block	1

04-12-2015-08:03:00 to 04-12-2015-09:03:00